Parlement européen
2019-2024

Commission de l'industrie, de la recherche et de l'énergie

2023/0109(COD)

22.9.2023

AMENDEMENTS
46 - 216

Projet de rapport
Lina Gálvez Muñoz
(PE752.795v01-00)

établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir

Proposition de règlement
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Amendement 46
Evžen Tošenovský

Proposition de règlement
Titre 1

Texte proposé par la Commission	*Amendement*
Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir ***(règlement sur la cybersolidarité)***

Or. en

Amendement 47
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Considérant 1

Texte proposé par la Commission	*Amendement*
(1) Le recours aux technologies de l'information et de la communication et la dépendance à l'égard de ces technologies sont désormais des aspects fondamentaux dans tous les secteurs d'activité économique, eu égard à l'interconnexion et à l'interdépendance sans précédent de nos administrations publiques, de nos entreprises et de nos citoyens par-delà les secteurs et les frontières.	(1) Le recours aux technologies de l'information et de la communication et la dépendance à l'égard de ces technologies sont désormais des aspects fondamentaux ***et des vulnérabilités*** dans tous les secteurs d'activité économique, eu égard à l'interconnexion et à l'interdépendance sans précédent de nos administrations publiques, de nos entreprises et de nos citoyens par-delà les secteurs et les frontières.

Or. en

Justification

La nécessité de ce texte juridique découle du fait que les dépendances fondamentales s'accompagnent également de vulnérabilités.

Amendement 48
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent	(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques ***dans l'ensemble de l'Union*** nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent

instantanément dans un grand nombre de pays.

simultanément ou se propagent instantanément dans un grand nombre de pays. ***Il est donc nécessaire d'instaurer une coopération étroite et coordonnée entre le secteur public, le secteur privé, les États membres, les institutions ou agences de l'Union et le milieu universitaire pour améliorer la posture de cybersécurité de l'Union européenne, laquelle devrait coordonner sa réaction avec les institutions internationales et les partenaires internationaux de confiance qui partagent les mêmes valeurs et l'aligner sur les cadres et accords de coopération internationale.***

Or. en

Amendement 49
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de	(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de

niveau étatique**,** criminels ***et hacktivistes*** qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays.	niveau étatique ***et des*** criminels qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays.

Or. en

Justification

Le fait d'assimiler l'hacktivisme à une activité criminelle ne rend pas compte de la diversité des activités concernées, parmi lesquelles figurent les protestations légitimes et les «faits de dénonciations». Il serait préférable que le texte évite les imprécisions et protège les activités légitimes.

Amendement 50
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareş Bogdan, Cristian-Silviu Buşoi

Proposition de règlement
Considérant 3

Texte proposé par la Commission	*Amendement*
(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent	(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent

trois propositions différentes de la conférence sur l'avenir de l'Europe[16], il convient d'accroître la résilience des citoyens, des entreprises et des entités exploitant des infrastructures critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures ***et*** des services qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité.

trois propositions différentes de la conférence sur l'avenir de l'Europe, il convient d'accroître la résilience des citoyens, des entreprises***, y compris les micro, petites et moyennes entreprises (PME),*** et des entités exploitant des infrastructures critiques***, notamment des autorités régionales et locales,*** face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures***,*** des services ***et du personnel hautement qualifié doté des compétences nécessaires*** qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir***, également en collectant des renseignements en amont***. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité. ***[1] https://futureu.europa.eu/en/***

---

[16] https://futureu.europa.eu/fr/

Or. en

Amendement 51
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 5

Texte proposé par la Commission	*Amendement*
(5) En raison de l'augmentation des risques liés à la cybersécurité et de la complexité globale du panorama des menaces, ainsi que du risque évident de	(5) En raison de l'augmentation des risques liés à la cybersécurité et de la complexité globale du panorama des menaces, ainsi que du risque évident de

propagation rapide des incidents de cybersécurité d'un État membre à un autre et d'un pays tiers à l'Union, il est nécessaire de renforcer la solidarité au niveau de l'UE afin de mieux détecter les menaces et incidents de cybersécurité, de s'y préparer ***et*** d'y réagir. Dans les conclusions du Conseil sur la posture cyber de l'Union, les États membres ont également invité la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité[21].	propagation rapide des incidents de cybersécurité d'un État membre à un autre et d'un pays tiers à l'Union, il est nécessaire de renforcer la solidarité au niveau de l'UE afin de mieux détecter les menaces et incidents de cybersécurité, de s'y préparer***,*** d'y réagir ***et de s'en rétablir***. Dans les conclusions du Conseil sur la posture cyber de l'Union, les États membres ont également invité la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité[21].
[21] Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne, approuvées par le Conseil lors de sa session du 23 mai 2022 (9364/22).	[21] Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne, approuvées par le Conseil lors de sa session du 23 mai 2022 (9364/22).

Or. en

Amendement 52
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 9 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(9 bis) À la lumière des évolutions géopolitiques et de l'intensification des cybermenaces, il est important d'assurer la continuité et le renforcement des mesures définies dans le présent règlement, en particulier en ce qui concerne le cyberbouclier européen et le mécanisme européen d'urgence dans le domaine de la cybersécurité. Il est donc nécessaire de prévoir une ligne budgétaire qui leur soit consacrée dans le cadre financier pluriannuel pour la période 2028-2034. Il convient également que les États membres s'engagent à soutenir toutes les mesures nécessaires pour renforcer la solidarité ainsi que pour

réduire les menaces et incidents de cybersécurité dans l'ensemble de l'Union.

Or. en

Amendement 53
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 12

Texte proposé par la Commission	*Amendement*
(12) Afin de prévenir, évaluer et contrer les menaces et incidents de cybersécurité de manière plus efficace, il est nécessaire d'acquérir des connaissances plus complètes sur les menaces qui pèsent sur les actifs et infrastructures critiques dans le territoire de l'Union, notamment leur répartition géographique, leur interconnexion et les effets potentiels de cyberattaques touchant ces infrastructures. Il convient de mettre en place une grande infrastructure de SOC à l'échelle de l'Union (le cyberbouclier européen), comprenant plusieurs plateformes transfrontières interopérables qui regroupent chacune plusieurs SOC nationaux. Une telle infrastructure devrait servir les intérêts et les besoins des États et de l'Union en matière de cybersécurité, en tirant parti de technologies de pointe pour la collecte et l'analyse avancées des données, en renforçant les capacités de détection et de gestion des incidents de cybersécurité et en permettant une appréciation de la situation en temps réel. Elle devrait également permettre d'améliorer la détection des menaces et incidents de cybersécurité, complétant et soutenant ainsi les entités et réseaux de l'Union chargés de la gestion de crise dans l'UE, notamment le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) tel que défini dans la	(12) Afin de prévenir, évaluer et contrer les menaces et incidents de cybersécurité de manière plus efficace, ***et s'en rétablir,*** il est nécessaire d'acquérir des connaissances plus complètes sur les menaces qui pèsent sur les actifs et infrastructures critiques dans le territoire de l'Union, notamment leur répartition géographique, leur interconnexion et les effets potentiels de cyberattaques touchant ces infrastructures***, y compris en collectant des renseignements en amont***. Il convient de mettre en place une grande infrastructure de SOC à l'échelle de l'Union (le cyberbouclier européen), comprenant plusieurs plateformes transfrontières interopérables qui regroupent chacune plusieurs SOC nationaux***. Un SOC national est une capacité centralisée chargée de la collecte continue de renseignements sur les menaces ainsi que de l'amélioration de la posture de cybersécurité des entités sous juridiction nationale par la prévention, la détection et l'analyse des menaces de cybersécurité***. Une telle infrastructure devrait servir les intérêts et les besoins des États et de l'Union en matière de cybersécurité, en tirant parti de technologies de pointe pour la collecte et l'analyse avancées des données, en renforçant les capacités de détection et de gestion des incidents de cybersécurité et en permettant une

directive (UE) 2022/2555 du Parlement européen et du Conseil[24].

appréciation de la situation en temps réel. Elle devrait également permettre d'améliorer la détection des menaces et incidents de cybersécurité, complétant et soutenant ainsi les entités et réseaux de l'Union chargés de la gestion de crise dans l'UE, notamment le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) tel que défini dans la directive (UE) 2022/2555 du Parlement européen et du Conseil[24].

[24] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

[24] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

Or. en

Amendement 54
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 13

Texte proposé par la Commission	*Amendement*
(13) Chaque État membre devrait désigner un organisme public au niveau national chargé de coordonner les activités de détection des cybermenaces sur son territoire. Ces SOC nationaux devraient servir de point de référence et d'accès au niveau national pour la participation au cyberbouclier européen et devraient veiller à ce que les informations relatives aux cybermenaces provenant d'entités publiques et privées soient partagées et collectées au niveau national de manière	(13) Chaque État membre devrait***, en vue de participer au cyberbouclier européen,*** désigner un organisme public au niveau national chargé de coordonner les activités de détection des cybermenaces ***et d'échange d'informations*** sur son territoire***. Les États membres sont vivement encouragés à intégrer la capacité du SOC national à leur structure et à leur gouvernance de cybersécurité existantes afin d'éviter tout doublon en matière de gouvernance et d'aligner le***

efficace et rationnelle.

règlement sur la cybersolidarité sur la législation existante, notamment sur la directive (UE) 2022/2555. Ces SOC nationaux devraient servir de point de référence et d'accès au niveau national pour la participation ***d'entités publiques et privées, notamment de leurs SOC,*** au cyberbouclier européen et devraient veiller à ce que les informations relatives aux cybermenaces provenant d'entités publiques et privées soient partagées et collectées au niveau national de manière efficace et rationnelle. ***Il convient que les SOC nationaux renforcent la coopération et le partage d'informations entre les entités publiques et privées afin de décloisonner la communication. Ils peuvent ainsi soutenir la création de modèles d'échange de données et devraient permettre et encourager le partage d'informations dans un environnement sûr et de confiance. Une coopération étroite et coordonnée entre les entités publiques et privées est essentielle pour renforcer la résilience de l'Union dans le domaine de la cybersécurité.***

Or. en

Amendement 55
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 14

Texte proposé par la Commission	*Amendement*
(14) Dans le cadre du cyberbouclier européen, il convient de créer un certain nombre de centres d'opérations de sécurité transfrontières (ci-après «SOC transfrontières»). Ceux-ci devraient regrouper les SOC nationaux d'au moins trois États membres afin de tirer pleinement parti des avantages de la	(14) Dans le cadre du cyberbouclier européen, il convient de créer un certain nombre de centres d'opérations de sécurité transfrontières (ci-après «SOC transfrontières»). Ceux-ci devraient regrouper les SOC nationaux d'au moins trois États membres afin de tirer pleinement parti des avantages de la

détection des menaces transfrontières ainsi que du partage et de la gestion des informations. L'objectif général des SOC transfrontières devrait être de renforcer les capacités d'analyse, de prévention et de détection des cybermenaces ainsi que de contribuer à l'obtention de renseignements de haute qualité sur les cybermenaces, notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées, à l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement de confiance. Ils devraient également apporter de nouvelles capacités supplémentaires, ***en s'appuyant sur*** les SOC ***existants***, ***sur*** les centres de réponse aux incidents de sécurité informatique (CSIRT) et ***sur*** d'autres acteurs pertinents***, et en les complétant***.

détection des menaces transfrontières ainsi que du partage et de la gestion des informations. L'objectif général des SOC transfrontières devrait être de renforcer les capacités d'analyse, de prévention et de détection des cybermenaces ainsi que de contribuer à l'obtention de renseignements de haute qualité sur les cybermenaces ***en amont***, notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées, à l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement de confiance. ***Les SOC transfrontières devraient permettre et encourager le partage d'informations dans un environnement sûr et sécurisé. L'ENISA devrait assister les SOC transfrontières sur les questions relatives à la coopération opérationnelle.*** Ils devraient également apporter de nouvelles capacités supplémentaires, ***venant s'intégrer à l'infrastructure de cybersécurité existante***, ***dont*** les SOC, les centres de réponse aux incidents de sécurité informatique (CSIRT) et d'autres acteurs pertinents.

Or. en

Amendement 56
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 15

Texte proposé par la Commission	*Amendement*
(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la	(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la

directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant ***compléter le*** réseau des CSIRT en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant au développement des capacités et de la souveraineté technologique de l'Union.

directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant ***s'intégrer à l'infrastructure de cybersécurité existante, en particulier au*** réseau des CSIRT***,*** en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées***, notamment de leur SOC***, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant au développement des capacités et de la souveraineté technologique de l'Union ***afin d'en renforcer la résilience***.

Or. en

Amendement 57
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Considérant 15

Texte proposé par la Commission	*Amendement*
(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant au développement ***des*** capacités ***et de la souveraineté technologique*** de l'Union.	(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant***, d'une part,*** au développement ***d'un important écosystème de cybersécurité doté de solides*** capacités de l'Union***, et, d'autre part, à la coopération avec des***

partenaires partageant nos valeurs.

Or. en

Amendement 58
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 16

Texte proposé par la Commission	*Amendement*
(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures critiques]. Les informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données issues de réseaux et de capteurs, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle.	(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures critiques]***, afin de favoriser le décloisonnement de la communication qui prévaut actuellement***. Les ***SOC transfrontières pourraient ainsi soutenir la création de modèles d'échange de données dans l'ensemble de l'Union. Les*** informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données issues de réseaux et de capteurs, des flux de renseignements sur les menaces, ***y compris des renseignements collectés en amont,*** des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle.

Or. en

Amendement 59
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Considérant 16

Texte proposé par la Commission	*Amendement*
(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures critiques]. Les informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données issues de réseaux ***et*** de capteurs, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle.	(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures critiques]. Les informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données ***analysées*** issues de réseaux***,*** de capteurs***, de la journalisation et de la télémesure***, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur ***les tactiques, techniques et procédures,*** les incidents***, les échantillons de logiciels malveillants***, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle.

Or. en

Amendement 60
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 17

Texte proposé par la Commission	*Amendement*

(17) Une appréciation de la situation commune aux autorités compétentes est un prérequis indispensable à la préparation et à la coordination en matière d'incidents de cybersécurité importants et majeurs à l'échelle de l'Union. La directive (UE) 2022/2555 a institué EU-CyCLONe afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. La recommandation (UE) 2017/1584 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs porte sur le rôle de tous les acteurs concernés. La directive (UE) 2022/2555 rappelle également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil, ainsi que sa responsabilité de fournir des rapports analytiques pour le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993. Par conséquent, lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos à EU-CyCLONe, au réseau des CSIRT et à la Commission. Selon les cas, ces informations à transmettre devraient comprendre plus particulièrement des informations techniques, des informations sur la nature et les motifs de l'attaquant ou de l'attaquant potentiel, ainsi que des informations non techniques de haut niveau sur tout incident de cybersécurité majeur potentiel ou en cours. Dans ce contexte, il convient de tenir dûment compte du besoin d'en connaître et du caractère potentiellement sensible des informations

(17) Une appréciation de la situation commune aux autorités compétentes est un prérequis indispensable à la préparation et à la coordination en matière d'incidents de cybersécurité importants et majeurs à l'échelle de l'Union. La directive (UE) 2022/2555 a institué EU-CyCLONe afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. La recommandation (UE) 2017/1584 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs porte sur le rôle de tous les acteurs concernés. La directive (UE) 2022/2555 rappelle également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil, ainsi que sa responsabilité de fournir des rapports analytiques pour le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993. Par conséquent, lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos à EU-CyCLONe, au réseau des CSIRT et à la Commission***, conformément aux dispositions existantes de la directive (UE) 2022/2555***. Selon les cas, ces informations à transmettre devraient comprendre plus particulièrement des informations techniques, des informations sur la nature et les motifs de l'attaquant ou de l'attaquant potentiel, ainsi que des informations non techniques de haut niveau sur tout incident de cybersécurité majeur potentiel ou en cours. Dans ce contexte, il convient de tenir dûment compte du besoin

transmises.

d'en connaître et du caractère potentiellement sensible des informations transmises.

Or. en

Amendement 61
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 19

Texte proposé par la Commission	*Amendement*
(19) Aux fins de l'échange des données sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement de confiance, les entités participant au cyberbouclier européen devraient être dotées d'outils, d'équipements et d'infrastructures de pointe hautement sécurisés. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données.	(19) Aux fins de l'échange des données sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement de confiance, les entités participant au cyberbouclier européen devraient être dotées d'outils, d'équipements et d'infrastructures de pointe hautement sécurisés***, ainsi que d'un personnel hautement qualifié***. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données.

Or. en

Amendement 62
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) En collectant, en partageant et en échangeant des données, le cyberbouclier	(20) En collectant, en partageant et en échangeant des données, le cyberbouclier

européen devrait renforcer la souveraineté technologique de l'Union. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].

européen devrait renforcer la souveraineté technologique de l'Union. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. ***Il convient toutefois de noter que l'intelligence artificielle se révèle plus efficace lorsqu'elle est couplée à l'analyse humaine. Le recours à un personnel hautement qualifié reste donc essentiel afin de mettre en commun des données de haute qualité et de collecter des renseignements sur les menaces en amont.*** Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].

[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).

[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).

Or. en

Amendement 63
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) En collectant, en partageant et en échangeant des données, le cyberbouclier européen devrait renforcer ***la souveraineté technologique*** de l'Union. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence	(20) En collectant, en partageant et en échangeant des données, le cyberbouclier européen devrait renforcer ***l'écosystème de cybersécurité considérable*** de l'Union. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées

artificielle et d'analyse des données. Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].

[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).

de l'intelligence artificielle et d'analyse des données. Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].

[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).

Or. en

Amendement 64
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Considérant 21

Texte proposé par la Commission	*Amendement*
(21) Bien que le cyberbouclier européen soit un projet civil, le renforcement des capacités civiles de détection et d'appréciation de la situation pour la protection des infrastructures critiques pourrait aussi profiter à la communauté de cyberdéfense. Les SOC transfrontières, avec le soutien de la Commission et du Centre de compétences européen en matière de cybersécurité (ECCC) et en coopération avec le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après le «haut représentant»), devraient progressivement élaborer des protocoles et des normes spécifiques afin de permettre une coopération avec la communauté de la cyberdéfense, y compris en ce qui concerne les conditions de vérification et de sécurité. La mise en place du cyberbouclier européen devrait s'accompagner d'une	(21) Bien que le cyberbouclier européen soit un projet civil, le renforcement des capacités civiles de détection et d'appréciation de la situation pour la protection des infrastructures critiques pourrait aussi profiter à la communauté de cyberdéfense. Les SOC transfrontières, avec le soutien de la Commission et du Centre de compétences européen en matière de cybersécurité (ECCC) et en coopération avec le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après le «haut représentant»), devraient progressivement élaborer des protocoles et des normes spécifiques ***en matière de conditions d'accès et de garanties*** afin de permettre une coopération avec la communauté de la cyberdéfense, y compris en ce qui concerne les conditions de vérification et de sécurité***, tout en respectant le caractère civil des***

réflexion qui permette une collaboration future avec les réseaux et plateformes de partage d'informations au sein de la communauté de cyberdéfense, en étroite coopération avec le haut représentant.	***institutions et la destination des financements, de sorte que les fonds mis à disposition de la communauté de défense soient utilisés***. La mise en place du cyberbouclier européen devrait s'accompagner d'une réflexion qui permette une collaboration future avec les réseaux et plateformes de partage d'informations au sein de la communauté de cyberdéfense, en étroite coopération avec le haut représentant ***et dans le plein respect des droits et des libertés***.

Or. en

Justification

Dans le souci d'éviter les doublons et de préserver les droits et les libertés, il convient de fonder la coopération entre les secteurs civil et militaire de la cybersécurité sur des garanties, en veillant à ne pas modifier la destination des financements civils.

Amendement 65
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 24

Texte proposé par la Commission	*Amendement*
(24) Compte tenu de l'augmentation des risques et du nombre d'incidents touchant les États membres, il est nécessaire de mettre en place un instrument de soutien en cas de crise visant à améliorer la résilience de l'Union face aux incidents de cybersécurité importants et majeurs et à compléter les mesures prises par les États membres au moyen d'une aide financière d'urgence destinée à la préparation, à la réaction et au rétablissement immédiat des services essentiels. Cet instrument devrait permettre de déployer rapidement de l'aide, dans des circonstances définies et des conditions claires, et permettre une surveillance et une évaluation minutieuses de l'utilisation des ressources. Si la	(24) Compte tenu de l'augmentation des risques et du nombre d'incidents touchant les États membres, il est nécessaire de mettre en place un instrument de soutien en cas de crise visant à améliorer la résilience de l'Union face aux incidents de cybersécurité importants et majeurs et à compléter les mesures prises par les États membres au moyen d'une aide financière d'urgence destinée à la préparation, à la réaction et au rétablissement immédiat des services essentiels. Cet instrument devrait permettre de déployer rapidement ***et efficacement*** de l'aide, dans des circonstances définies et des conditions claires, et permettre une surveillance et une évaluation minutieuses de l'utilisation des

responsabilité première en matière de prévention, de préparation et de réaction face aux incidents et aux crises de cybersécurité incombe aux États membres, le mécanisme d'urgence dans le domaine de la cybersécurité promeut la solidarité entre les États membres, conformément à l'article 3, paragraphe 3, du traité sur l'Union européenne (TUE).	ressources. Si la responsabilité première en matière de prévention, de préparation et de réaction face aux incidents et aux crises de cybersécurité incombe aux États membres, le mécanisme d'urgence dans le domaine de la cybersécurité promeut la solidarité entre les États membres, conformément à l'article 3, paragraphe 3, du traité sur l'Union européenne (TUE).

Or. en

Amendement 66
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 27

Texte proposé par la Commission	*Amendement*
(27) L'aide apportée dans le cadre du présent règlement devrait appuyer et compléter les mesures prises par les États membres au niveau national. À cette fin, il est nécessaire d'assurer une coopération et une consultation étroites entre la Commission et les États membres touchés. Lorsqu'un État membre sollicite une aide au titre du mécanisme d'urgence dans le domaine de la cybersécurité, il devrait fournir des informations pertinentes permettant de justifier sa demande aide.	(27) L'aide apportée dans le cadre du présent règlement devrait appuyer et compléter les mesures prises par les États membres au niveau national. À cette fin, il est nécessaire d'assurer une coopération et une consultation étroites entre la Commission***, l'ENISA*** et les États membres touchés. Lorsqu'un État membre sollicite une aide au titre du mécanisme d'urgence dans le domaine de la cybersécurité, il devrait fournir des informations pertinentes permettant de justifier sa demande aide.

Or. en

Amendement 67
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 33

Texte proposé par la Commission	*Amendement*
(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle devrait comprendre des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, dans des conditions similaires.	(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle devrait comprendre des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services***, tout en renforçant la résilience et la compétitivité de l'Union, notamment la participation de fournisseurs européens de services de sécurité gérés qui sont des PME. Les fournisseurs de confiance, dont les PME, devraient pouvoir coopérer les uns avec les autres afin de satisfaire aux critères susmentionnés***. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national***. Dans la mesure du possible, les services devraient se fonder sur des technologies de pointe, notamment l'informatique en nuage et l'intelligence artificielle. Il convient donc que la réserve de cybersécurité incite à investir dans la recherche et l'innovation afin d'encourager le développement de ces technologies. Le cas échéant, des exercices communs réunissant les fournisseurs de confiance et les utilisateurs potentiels de la réserve de cybersécurité pourraient être menés afin de garantir le bon fonctionnement de la réserve***. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions,

organes ou organismes de l'Union, dans des conditions similaires.

Or. en

Amendement 68
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Considérant 33

Texte proposé par la Commission	*Amendement*
(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle ***devrait comprendre*** des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, dans des conditions similaires.	(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement ***et recevoir un financement initial de 10 millions d'EUR en vertu du présent règlement en attendant l'évaluation.*** Elle ***comprend*** des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, dans des conditions similaires. ***La Commission veille à éviter tout doublon avec des initiatives similaires menées au sein de l'OTAN.***

Or. en

Justification

La Commission prévoit une «mise en place progressive» de la réserve, mais le reste de la proposition de règlement fait l'impasse sur ce point. Cet amendement propose donc de réduire le budget initial de la réserve de 36 millions à 10 millions d'EUR jusqu'à ce que le présent règlement fasse l'objet d'une évaluation. Ainsi, 26 millions d'EUR pourraient être restitués au programme pour une Europe numérique, notamment à son objectif spécifique 4 sur les compétences numériques avancées (sur les 35 millions qui lui ont été soustraits). La création d'une réserve de cybersécurité de l'Union qui viendrait compléter la réserve de cybersécurité de l'OTAN présente un risque élevé de doublons et ne devrait pas se faire au détriment d'un investissement plus important dans les efforts visant à attirer et à faire progresser les talents dans le domaine de la cybersécurité en Europe.

Amendement 69
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 35

Texte proposé par la Commission	*Amendement*
(35) Aux fins de la mise en place de la réserve de cybersécurité de l'UE, la Commission ***pourrait envisager de*** demander à l'ENISA de préparer un schéma de certification candidat, conformément au règlement (UE) 2019/881, pour les services de sécurité gérés dans les domaines couverts par le mécanisme d'urgence dans le domaine de la cybersécurité.	(35) Aux fins de la mise en place de la réserve de cybersécurité de l'UE, la Commission ***devrait*** demander à l'ENISA de préparer un schéma de certification candidat, conformément au règlement (UE) 2019/881, pour les services de sécurité gérés dans les domaines couverts par le mécanisme d'urgence dans le domaine de la cybersécurité.

Or. en

Amendement 70
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Proposition de règlement
Considérant 35 bis (nouveau)

Texte proposé par la Commission	*Amendement*

(35 bis) Au vu des tâches supplémentaires prévues dans le présent règlement ainsi que dans la [proposition concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques], il convient de doter l'ENISA des ressources financières et humaines nécessaires dans le cadre du budget de l'Union.

Or. en

Amendement 71
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 37 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(37 bis) Les fournisseurs de services de réaction aux incidents de pays tiers, notamment de pays tiers associés au programme pour une Europe numérique, de pays membres de l'OTAN ou d'autres pays partenaires internationaux partageant les mêmes valeurs, peuvent jouer un rôle utile pour ce qui est de fournir des services spécifiques au sein de la réserve de cybersécurité de l'Union. Il peut s'avérer nécessaire de limiter la participation d'entités juridiques établies dans des pays non associés ou contrôlées par ceux-ci, ou de les en exclure, afin de renforcer la résilience et la souveraineté de l'Union ainsi que de protéger ses actifs stratégiques, ses intérêts ou sa sécurité.

Or. en

Amendement 72
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 38 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(38 bis) Il est impératif de disposer d'un personnel hautement qualifié capable de fournir les services de cybersécurité pertinents de manière fiable et dans le respect des normes les plus rigoureuses, afin de garantir le déploiement efficace du cyberbouclier européen et du mécanisme d'urgence dans le domaine de la cybersécurité. Il y a donc lieu de se préoccuper de la pénurie de talents dont souffre l'Union, qui se caractérise par le manque de professionnels qualifiés, alors qu'elle doit faire face à un panorama de menaces en constante évolution, comme le reconnaît la Commission dans sa communication du 18 avril 2023 sur l'Académie des compétences en matière de cybersécurité. Il importe de remédier à cette pénurie de talents en renforçant la coopération et la coordination entre les différentes parties prenantes, notamment le secteur privé, les milieux universitaires, les États membres, la Commission et l'ENISA, afin d'intensifier et de créer des synergies en faveur des investissements dans l'éducation et la formation, du développement de partenariats public-privé, du soutien aux initiatives de recherche et d'innovation, de l'élaboration et de la reconnaissance mutuelle de normes communes et de la certification des compétences dans le domaine de la cybersécurité, y compris au moyen du cadre européen de certification de cybersécurité. Cette mesure devrait également permettre de faciliter la mobilité des professionnels de la cybersécurité au sein de l'Union. Le présent règlement devrait viser à promouvoir une main-d'œuvre plus diversifiée dans le domaine de la cybersécurité.

Or. en

Amendement 73
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 38 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(38 ter) Le renforcement des capacités des États membres est essentiel pour assurer une approche coordonnée à l'échelle de l'Union visant à améliorer la résilience de sa posture de cybersécurité. Comme l'a souligné la Commission dans sa communication du 18 avril 2023 sur l'Académie des compétences en matière de cybersécurité, la sécurité de l'Union ne peut pas être assurée sans son atout le plus précieux, à savoir sa population. Le cadre européen de certification de cybersécurité peut contribuer à une meilleure compréhension de la composition de la main-d'œuvre de l'Union, notamment des compétences actuelles et recherchées chez les entités participantes.

Or. en

Amendement 74
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Considérant 39

Texte proposé par la Commission	*Amendement*
(39) L'objectif poursuivi par le présent règlement peut être mieux atteint au niveau de l'Union que par les États membres. En conséquence, l'Union peut adopter des	(39) L'objectif poursuivi par le présent règlement***, à savoir le décloisonnement de la communication et le renforcement des capacités de prévention, de détection, de***

mesures conformément aux principes de subsidiarité et de proportionnalité énoncés à l'article 5 du traité sur l'Union européenne. Le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif,

réaction et de rétablissement, peut être mieux atteint au niveau de l'Union que par les États membres. En conséquence, l'Union peut adopter des mesures conformément aux principes de subsidiarité et de proportionnalité énoncés à l'article 5 du traité sur l'Union européenne. Le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif,

Or. en

Amendement 75
Nicola Danti

Proposition de règlement
Considérant 39 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(39 bis) Au vu des tâches supplémentaires prévues dans le présent règlement ainsi que dans la [proposition concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques], il convient de doter l'ENISA des ressources financières et humaines nécessaires dans le cadre du budget de l'Union.

Or. en

Amendement 76
Johan Nissinen

Proposition de règlement
Article 1 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. Le présent règlement établit des mesures destinées à renforcer les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y	1. ***Tout en reconnaissant que la sécurité nationale, en particulier dans le domaine de la cybersécurité, reste de la seule responsabilité de chaque État***

préparer et d'y réagir, notamment par les actions suivantes:	***membre,*** le présent règlement établit des mesures destinées à renforcer les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, notamment par les actions suivantes:

Or. en

Amendement 77
Evžen Tošenovský

Proposition de règlement
Article 1 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) le déploiement ***d'une infrastructure paneuropéenne*** de centres d'opérations de sécurité («***cyberbouclier européen***») dans le but de mettre en place et de développer des capacités communes de détection et d'appréciation de la situation;	a) le ***renforcement des centres de réponse aux incidents de sécurité informatiques (CSIRT) visés à l'article 10 de la directive (UE) 2022/2555, et du réseau des CSIRT visé à l'article 15 de la directive (UE) 2022/2555, ainsi que le*** déploiement de centres d'opérations de sécurité («***SOC***») dans le but de mettre en place et de développer des capacités communes ***et nationales*** de détection et d'appréciation de la situation ***(«cyberbouclier européen»)***;

Or. en

Amendement 78
Evžen Tošenovský

Proposition de règlement
Article 1 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) la mise en place d'un mécanisme européen d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents importants ou majeurs.	***supprimé***

Or. en

Amendement 79
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la souveraineté technologique de l'Union dans le domaine de la cybersécurité;	a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie***, y compris les PME,*** et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la souveraineté technologique de l'Union dans le domaine de la cybersécurité;

Or. en

Amendement 80
Johan Nissinen

Proposition de règlement
Article 1 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la souveraineté technologique de l'Union dans le domaine de la cybersécurité;	a) renforcer la détection et l'appréciation de la situation communes ***volontaires*** au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la souveraineté technologique de l'Union dans le domaine de la cybersécurité;

Or. en

Amendement 81
Johan Nissinen

Proposition de règlement
Article 1 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la ***solidarité*** en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité;	b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la ***coopération volontaire*** en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité;

Or. en

Amendement 82
Evžen Tošenovský

Proposition de règlement
Article 1 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) augmenter la résilience de l'Union et contribuer à une réaction efficace en analysant et en évaluant les incidents importants ou majeurs, y compris en tirant les enseignements de l'expérience acquise et, le cas échéant, en formulant des recommandations.	***supprimé***

Or. en

Amendement 83
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 1 – paragraphe 2 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) renforcer et améliorer, de manière coordonnée, les aptitudes et les compétences de la main-d'œuvre dans le secteur de la cybersécurité, en travaillant en étroite coopération avec l'académie des compétences en matière de cybersécurité afin de dispenser des formations et donner des possibilités dans le but de remédier au déficit de talents dans le secteur de la cybersécurité.

Or. en

Amendement 84
Johan Nissinen

Proposition de règlement
Article 1 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Le présent règlement est sans préjudice de la responsabilité première des États membres dans le domaine de la sécurité nationale, de la sécurité publique, de la prévention et de la détection des infractions pénales et d'enquêtes et de poursuites en la matière.	3. Le présent règlement est sans préjudice de la responsabilité première des États membres dans le domaine de la sécurité nationale, de la sécurité publique, de la prévention et de la détection des infractions pénales et d'enquêtes et de poursuites en la matière***, et évite de faire double emploi avec des initiatives existantes***.

Or. en

Amendement 85
Evžen Tošenovský

Proposition de règlement
Article 1 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Le présent règlement est sans préjudice de la ***responsabilité première*** des États membres dans le domaine de la sécurité nationale, de la sécurité publique, de la prévention et de la détection des infractions pénales et d'enquêtes et de poursuites en la matière.	3. Le présent règlement est sans préjudice de la ***compétence exclusive*** des États membres dans le domaine de la sécurité nationale, de la sécurité publique, de la prévention et de la détection des infractions pénales et d'enquêtes et de poursuites en la matière.

Or. en

Amendement 86
Nicola Danti

Proposition de règlement
Article 1 – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis. Chaque année, lors de la présentation du projet de budget pour l'année suivante, la Commission soumet une évaluation détaillée des tâches confiées à l'ENISA en vertu du présent règlement et de la [proposition de règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques], ainsi que d'autres textes législatifs de l'Union, et précise les ressources financières et humaines nécessaires à l'accomplissement de ces tâches.

Or. en

Amendement 87
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
1) «centre d'opérations de sécurité transfrontière» («SOC transfrontière»): une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, les SOC nationaux d'au moins trois États membres qui forment un consortium d'hébergement, et qui est conçue pour prévenir les cybermenaces et les incidents et pour soutenir la production de renseignements de haute qualité, notamment par l'échange de données provenant de différentes sources, publiques et privées, ainsi que par le partage d'outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance; «organisme public»:	***supprimé***

Or. en

Amendement 88
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 2 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
1) «centre d'opérations de sécurité transfrontière» («SOC transfrontière»): une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, les SOC nationaux d'au moins trois États membres qui forment un consortium d'hébergement, et qui est conçue pour ***prévenir*** les cybermenaces et les incidents ***et*** pour soutenir la production de renseignements de haute qualité, notamment par l'échange de données provenant de différentes sources, publiques et privées, ainsi que par le partage d'outils de pointe et le développement conjoint de	1) «centre d'opérations de sécurité transfrontière» («SOC transfrontière»): une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, les SOC nationaux d'au moins trois États membres qui forment un consortium d'hébergement, et qui est conçue pour ***détecter et analyser*** les cybermenaces et ***prévenir*** les incidents***, de même que*** pour soutenir la production de renseignements de haute qualité, notamment par l'échange de données provenant de différentes sources, publiques et privées, ainsi que par le partage d'outils

capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance; «organisme public»:

de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance; «organisme public»:

Or. en

Amendement 89
Johan Nissinen

Proposition de règlement
Article 2 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
1) «centre d'opérations de sécurité transfrontière» («SOC transfrontière»): une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, les SOC nationaux d'au moins trois États membres qui forment un consortium d'hébergement, et qui est conçue pour prévenir les cybermenaces et les incidents et pour soutenir la production de renseignements de haute qualité, notamment par l'échange de données provenant de différentes sources, publiques et privées, ainsi que par le partage d'outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance; «organisme public»:	1) «centre d'opérations de sécurité transfrontière» («SOC transfrontière»): une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, les SOC nationaux d'au moins trois États membres qui forment un consortium d'hébergement, et qui est conçue pour prévenir les cybermenaces et les incidents et pour soutenir la production de renseignements de haute qualité, notamment par l'échange ***volontaire*** de données provenant de différentes sources, publiques et privées, ainsi que par le partage d'outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance; «organisme public»:

Or. en

Amendement 90
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 2 – alinéa 1 – point 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis) «centre d'opérations de sécurité» («SOC»): une capacité centralisée, en interne ou sous-traitée, chargée du suivi et de l'amélioration continus de la posture de cybersécurité d'une entité en vue de prévenir et de détecter les menaces de cybersécurité, de les analyser et d'y réagir.

Or. en

Amendement 91
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis) «centre d'opérations de sécurité» («SOC»): un centre mis en place par une entité, privée ou publique, ou par une autorité nationale, qui assure le suivi et l'analyse continus des réseaux de communication et des systèmes informatiques afin de détecter les intrusions et les anomalies en temps réel.

Or. en

Amendement 92
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 2 – alinéa 1 – point 1 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	1 ter) «centre d'opérations de sécurité national» («SOC national»): une capacité centralisée chargée de la collecte continue de renseignements sur les menaces et de

l'amélioration de la posture de cybersécurité des entités sous juridiction nationale par la prévention, la détection et l'analyse des menaces de cybersécurité afin de pouvoir mieux réagir aux menaces de cybersécurité. Cette capacité est, le cas échéant, intégrée aux structures nationales déjà existantes, telles que les CSIRT établis en vertu de la directive (UE) 2022/2555.

Or. en

Amendement 93
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 2

Texte proposé par la Commission	*Amendement*
2)() «***organisme public***»: ***un organisme de droit public*** au sens de l'article ***2, paragraphe 1***, point ***4)***, de la directive ***2014/24/UE du Parlement européen et du Conseil***[30];	2) «***entité de l'administration publique***»: ***une entité de l'administration publique*** au sens de l'article ***6***, point ***35***), de la directive ***(UE) 2022/2555***;

[30] Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

Or. en

Amendement 94
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 3

Texte proposé par la Commission	*Amendement*
3) «consortium d'hébergement»: un	***supprimé***

consortium formé par des États participants, représentés par les SOC nationaux, qui ont accepté de mettre en place un SOC transfrontière et de contribuer à l'acquisition des outils et de l'infrastructure nécessaires à ce centre, ainsi qu'au fonctionnement de celui-ci;

Or. en

Amendement 95
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis) «traitement des incidents»: le traitement des incidents au sens de l'article 6, point 8), de la directive (UE) 2022/2555;

Or. en

Amendement 96
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 5 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	5 ter) «risque»: un risque au sens de l'article 6, point 9), de la directive (UE) 2022/2555;

Or. en

Amendement 97
Evžen Tošenovský

Proposition de règlement

Article 2 – alinéa 1 – point 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis) «cybermenace importante»: une cybermenace au sens de l'article 6, point 11), de la directive (UE) 2022/2555;

Or. en

Amendement 98
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 9

Texte proposé par la Commission	*Amendement*
9) «préparation»: un état de préparation et une capacité d'assurer une réaction rapide et efficace à un incident de cybersécurité important ou majeur, résultant d'une évaluation des risques et de mesures de surveillance prises à l'avance;	***supprimé***

Or. en

Amendement 99
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 10

Texte proposé par la Commission	*Amendement*
10) «réaction»: une action en cas d'incident de cybersécurité important ou majeur, ou pendant ou après un tel incident, menée afin de faire face à ses conséquences négatives immédiates et à court terme;	***supprimé***

Or. en

Amendement 100
Evžen Tošenovský

Proposition de règlement
Article 2 – alinéa 1 – point 11

Texte proposé par la Commission	*Amendement*
11) «fournisseurs de confiance»: les fournisseurs de services de sécurité gérés au sens de l'article 6, point 40), de la directive (UE) 2022/2555 sélectionnés conformément à l'article 16 du présent règlement.	11) «fournisseurs ***de services de sécurité gérés*** de confiance»: les fournisseurs de services de sécurité gérés au sens de l'article 6, point 40), de la directive (UE) 2022/2555 sélectionnés ***en vue d'être inclus dans la réserve de cybersécurité de l'Union*** conformément à l'article 16 du présent règlement.

Or. en

Amendement 101
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 3 – paragraphe 1 – alinéa 1

Texte proposé par la Commission	*Amendement*
Une infrastructure paneuropéenne interconnectée de centres d'opérations de sécurité («cyberbouclier européen») est mise en place pour doter l'Union de capacités avancées lui permettant de détecter, d'analyser et de traiter des données sur les cybermenaces ***et*** les incidents sur son territoire. Elle est formée par l'ensemble des centres d'opérations de sécurité nationaux («SOC nationaux») et des centres d'opérations de sécurité transfrontières («SOC transfrontières»).	Une infrastructure paneuropéenne interconnectée de centres d'opérations de sécurité («cyberbouclier européen») est mise en place pour doter l'Union de capacités avancées lui permettant de détecter, d'analyser et de traiter des données sur les cybermenaces ***ainsi que de prévenir*** les incidents sur son territoire. Elle est formée par l'ensemble des centres d'opérations de sécurité nationaux («SOC nationaux») et des centres d'opérations de sécurité transfrontières («SOC transfrontières»).

Or. en

Amendement 102
Johan Nissinen

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
a) met en commun et partage, par ***l'intermédiaire*** des SOC transfrontières, des données sur les cybermenaces et les incidents provenant de différentes sources;	a) met en commun et partage, par ***l'échange volontaire d'informations provenant*** des SOC transfrontières, des données sur les cybermenaces et les incidents provenant de différentes sources;

Or. en

Amendement 103
Evžen Tošenovský

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
a) met en commun et partage, par l'intermédiaire des SOC transfrontières, des données sur les cybermenaces et les incidents provenant de différentes sources;	a) met en commun et partage, par l'intermédiaire des SOC transfrontières, des données sur les cybermenaces et les incidents provenant de différentes sources***, tant au niveau national qu'au niveau de l'Union***;

Or. en

Amendement 104
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point c

Texte proposé par la Commission	*Amendement*
c) contribue à améliorer la protection contre les cybermenaces et la réaction face à celles-ci;	c) contribue à améliorer la protection contre les cybermenaces et la réaction face à celles-ci***, notamment en formulant des***

	recommandations concrètes à l'intention des entités;

Or. en

Amendement 105
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
d) participe à une détection plus rapide des cybermenaces et à l'appréciation de la situation dans l'ensemble de l'Union;	d) participe à une détection plus rapide des cybermenaces et à l'appréciation de la situation dans l'ensemble de l'Union***, notamment en collectant des renseignements en amont***;

Or. en

Amendement 106
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point e

Texte proposé par la Commission	*Amendement*
e) fournit des services et des activités à la communauté de la cybersécurité dans l'Union, y compris en contribuant au développement d'outils avancés d'intelligence artificielle et d'analyse de données.	*(Ne concerne pas la version française.)*

Or. en

Amendement 107
Evžen Tošenovský

Proposition de règlement

Article 4 – titre

Texte proposé par la Commission	*Amendement*
Centres d'opérations de sécurité nationaux	***Renforcement de la coopération et de l'échange d'informations au niveau national***

Or. en

Amendement 108
Evžen Tošenovský

Proposition de règlement
Article 4 – paragraphe 1 – alinéa 1

Texte proposé par la Commission	*Amendement*
Chaque État membre désigne ***au moins un SOC national*** en vue de ***participer*** au cyberbouclier européen***. Le SOC national est un organisme public***.	Chaque État membre désigne ***l'un de ses centres de réponse aux incidents de sécurité informatiques (CSIRT), visés à l'article 10 de la directive (UE) 2022/2555, en tant que centre d'échange et d'analyse d'informations (ISAC)*** en vue de ***contribuer*** au cyberbouclier européen.

Or. en

Amendement 109
Evžen Tošenovský

Proposition de règlement
Article 4 – paragraphe 1 – alinéa 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Les organisations privées et publiques ou les autorités nationales, en particulier les entités actives dans des secteurs critiques ou hautement critiques, sont encouragées à établir et à gérer leurs propres SOC, autonomes ou communs.

Or. en

Amendement 110
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 4 – paragraphe 1 – alinéa 2

Texte proposé par la Commission	*Amendement*
Il peut servir de point de référence et d'accès à d'autres organisations publiques et privées au niveau national pour collecter et analyser des informations sur les menaces ***et incidents*** de cybersécurité et contribuer aux travaux d'un SOC transfrontière. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité.	Il peut servir de point de référence et d'accès à d'autres organisations publiques et privées au niveau national pour collecter et analyser des informations sur les menaces de cybersécurité et contribuer aux travaux d'un SOC transfrontière. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité. ***Le SOC ou le CSIRT national peut demander aux fournisseurs de confiance ou aux fournisseurs de services de sécurité gérés de lui fournir des données de télémesure, de capteurs ou de journalisation ayant trait à des secteurs hautement critiques, au sens de la directive (UE) 2022/2555. Le partage de ces données ne peut être effectué qu'afin de soutenir les tâches et les responsabilités du SOC ou du CSIRT national consistant à détecter et à prévenir les incidents de cybersécurité.***

Or. en

Amendement 111
Evžen Tošenovský

Proposition de règlement
Article 4 – paragraphe 1 – alinéa 2

Texte proposé par la Commission	*Amendement*
Il peut servir de point de référence et d'accès ***à*** d'autres organisations publiques et privées au niveau national pour collecter et analyser des informations sur les	Il peut servir de point de référence et d'accès ***principalement aux SOC relevant d'entités publiques ou privées ou d'une autorité nationale, aux autres CSIRT du***

menaces et incidents de cybersécurité ***et contribuer aux travaux d'un SOC transfrontière***. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité***.***	***même État membre, au coordinateur responsable de la gestion des incidents et des crises de cybersécurité majeurs, ainsi qu'à*** d'autres organisations publiques et privées au niveau national pour collecter et analyser des informations sur les menaces et incidents de cybersécurité ***et, le cas échéant, pour échanger ces informations avec d'autres membres du réseau des CSIRT***. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité.

Or. en

Amendement 112
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 4 – paragraphe 1 – alinéa 2

Texte proposé par la Commission	*Amendement*
Il peut servir de point de référence et d'accès à d'autres organisations publiques et privées au niveau national pour collecter et analyser des informations sur les menaces et incidents de cybersécurité et contribuer aux travaux d'un SOC transfrontière. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité.	Il peut servir de point de référence et d'accès à d'autres organisations publiques et privées au niveau national***, en particulier à leur SOC,*** pour collecter et analyser des informations sur les menaces et incidents de cybersécurité et contribuer aux travaux d'un SOC transfrontière. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité.

Or. en

Amendement 113
Evžen Tošenovský

Proposition de règlement
Article 4 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux sont sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.	***supprimé***

Or. en

Amendement 114
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Article 4 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux ***sont*** sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et infrastructures. La contribution financière	2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux ***peuvent être*** sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et infrastructures. La contribution financière

de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.	de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.

Or. en

Justification

Le caractère obligatoire de la formulation aboutit à vider de leur contenu les principes d'appel à manifestation d'intérêt et de processus de sélection. Il va de soi que les SOC peuvent participer et être sélectionnés.

Amendement 115
Evžen Tošenovský

Proposition de règlement
Article 4 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Un SOC national sélectionné conformément au paragraphe 2 s'engage à demander à participer à un SOC transfrontière dans un délai de deux ans à compter de la date d'acquisition des outils et infrastructures ou de la date à laquelle il reçoit une subvention, selon ce qui se produit plus tôt. Si, à l'expiration de ce délai, le SOC national n'est pas devenu un participant à un SOC transfrontière, il ne pourra pas bénéficier d'un soutien supplémentaire de l'Union au titre du présent règlement.	***supprimé***

Or. en

Amendement 116

Evžen Tošenovský

Proposition de règlement
Article 5 – titre

Texte proposé par la Commission	*Amendement*
Centres d'opérations de sécurité transfrontières	***Acquisition conjointe d'outils et d'infrastructures***

Or. en

Amendement 117
Evžen Tošenovský

Proposition de règlement
Article 5 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Un consortium d'hébergement composé d'au moins trois États membres, représentés par des SOC nationaux, résolus à collaborer pour coordonner leurs activités de détection des incidents de cybersécurité et de surveillance des cybermenaces, peut participer à des actions visant à mettre en place un SOC transfrontière.	***supprimé***

Or. en

Amendement 118
Evžen Tošenovský

Proposition de règlement
Article 5 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. À la suite d'un appel à manifestation d'intérêt, un ***consortium d'hébergement est*** sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre.	2. À la suite d'un appel à manifestation d'intérêt, un ***CSIRT-ISAC peut être*** sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre.

L'ECCC peut octroyer au ***consortium d'hébergement*** une subvention destinée à financer le fonctionnement des outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par le ***consortium d'hébergement***. Avant de lancer la procédure d'acquisition des outils et infrastructures, l'ECCC et le ***consortium d'hébergement concluent*** une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.	L'ECCC peut octroyer au ***CSIRT-ISAC*** une subvention destinée à financer le fonctionnement des outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par le ***CSIRT-ISAC***. Avant de lancer la procédure d'acquisition des outils et infrastructures, l'ECCC et le ***CSIRT-ISAC participant conclut*** une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures***, y compris leur utilisation par d'autres CSIRT et SOC dans cet État membre***.

Or. en

Amendement 119
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Article 5 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. À la suite d'un appel à manifestation d'intérêt, un consortium d'hébergement ***est*** sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer au consortium d'hébergement une subvention destinée à financer le fonctionnement des outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par le consortium d'hébergement. Avant de lancer la procédure d'acquisition des outils et infrastructures, l'ECCC et le consortium d'hébergement concluent une convention d'hébergement et d'utilisation qui régit	2. À la suite d'un appel à manifestation d'intérêt, un consortium d'hébergement ***peut être*** sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer au consortium d'hébergement une subvention destinée à financer le fonctionnement des outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par le consortium d'hébergement. Avant de lancer la procédure d'acquisition des outils et infrastructures, l'ECCC et le consortium d'hébergement concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et

l'utilisation des outils et infrastructures.	infrastructures.

Or. en

Justification

Si le présent règlement n'inclut pas de critères précis, d'autres législations applicables sont quant à elles susceptibles de réduire la certitude d'un ou des candidats de se voir sélectionnés.

Amendement 120
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 5 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Toute entité privée établie dans un pays tiers partageant nos valeurs devrait être en mesure de participer à une procédure d'acquisition, à condition que cela ne soit pas contraire aux intérêts de l'Union et des États membres en matière de sécurité et de défense tels qu'ils sont définis dans le cadre de la PESC en application du titre V du traité sur l'Union européenne, ni aux objectifs énoncés à l'article 3 du présent règlement. Ces entités privées ne devraient pas être contrôlées par un pays tiers non associé, auquel cas elles font l'objet d'un filtrage au sens du règlement (UE) 2019/452 du Parlement européen et du Conseil.

Or. en

Amendement 121
Evžen Tošenovský

Proposition de règlement
Article 5 – paragraphe 3

Texte proposé par la Commission	*Amendement*

3. Les membres du consortium d'hébergement concluent un accord de consortium écrit qui définit les modalités internes de mise en œuvre de la convention d'hébergement et d'utilisation.	***supprimé***

Or. en

Amendement 122
Evžen Tošenovský

Proposition de règlement
Article 5 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Un SOC transfrontière est représenté à des fins juridiques par un SOC national agissant en tant que SOC coordinateur, ou par le consortium d'hébergement s'il est doté de la personnalité juridique. Le SOC coordinateur est responsable du respect des exigences prévues dans la convention d'hébergement et d'utilisation et dans le présent règlement.	***supprimé***

Or. en

Amendement 123
Evžen Tošenovský

Proposition de règlement
Article 6 – titre

Texte proposé par la Commission	*Amendement*
Coopération et partage d'informations ***au sein des SOC transfrontières et entre ceux-ci***	***Renforcement de la*** coopération et ***du*** partage d'informations ***au niveau de l'Union***

Or. en

Amendement 124
Johan Nissinen

Proposition de règlement
Article 6 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. Les membres d'un consortium d'hébergement ***s'échangent*** des informations pertinentes au sein du SOC transfrontière, y compris des informations sur les cybermenaces, les incidents évités, les vulnérabilités, les techniques et les procédures, les indicateurs de compromission, les tactiques adverses, les informations spécifiques sur les acteurs de la menace, les alertes de cybersécurité et les recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:	1. Les membres d'un consortium d'hébergement ***peuvent s'échanger*** des informations pertinentes au sein du SOC transfrontière, y compris des informations sur les cybermenaces, les incidents évités, les vulnérabilités, les techniques et les procédures, les indicateurs de compromission, les tactiques adverses, les informations spécifiques sur les acteurs de la menace, les alertes de cybersécurité et les recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

Or. en

Amendement 125
Evžen Tošenovský

Proposition de règlement
Article 6 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. Les ***membres d'un consortium d'hébergement*** s'échangent des informations pertinentes au sein du ***SOC transfrontière***, y compris des informations sur les cybermenaces, les incidents évités, les vulnérabilités, les techniques et les procédures, les indicateurs de compromission, les tactiques adverses, les informations spécifiques sur les acteurs de la menace, les alertes de cybersécurité et les recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:	1. Les ***CSIRT-ISAC et les autres CSIRT*** s'échangent des informations pertinentes au sein du ***réseau des CSIRT***, y compris des informations sur les cybermenaces, les incidents évités, les vulnérabilités, les techniques et les procédures, les indicateurs de compromission, les tactiques adverses, les informations spécifiques sur les acteurs de la menace, les alertes de cybersécurité et les recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

Or. en

Amendement 126
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 6 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) ***vise à*** prévenir ***et à*** détecter les incidents, ***à y réagir, à s'en rétablir ou à atténuer leur impact***;	a) ***améliore l'échange de renseignements sur les cybermenaces entre les SOC et le secteur des ISAC dans le but de*** prévenir***, de*** détecter ***et d'atténuer*** les incidents;

Or. en

Amendement 127
Evžen Tošenovský

Proposition de règlement
Article 6 – paragraphe 2 – partie introductive

Texte proposé par la Commission	*Amendement*
2. L'accord ***de consortium écrit visé à l'article 5***, ***paragraphe 3, établit***:	2. L'accord ***d'échange d'informations et de renseignements entre les CSIRT-ISAC ou, le cas échéant, d'autres CSIRT***, ***peut établir***:

Or. en

Amendement 128
Johan Nissinen

Proposition de règlement
Article 6 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) un engagement de partager ***une quantité importante de*** données visées au paragraphe 1 et les conditions dans	a) un engagement de partager ***volontairement les*** données visées au paragraphe 1 et les conditions dans

lesquelles ces informations doivent être échangées;	lesquelles ces informations doivent être échangées;

Or. en

Amendement 129
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 6 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) un engagement de partager ***une quantité importante de*** données visées au paragraphe 1 et les conditions dans lesquelles ces informations doivent être échangées;	a) un engagement de partager ***les*** données ***significatives*** visées au paragraphe 1 et les conditions dans lesquelles ces informations doivent être échangées;

Or. en

Amendement 130
Evžen Tošenovský

Proposition de règlement
Article 6 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Afin d'encourager l'échange d'informations entre les SOC transfrontières, ces derniers garantissent un niveau élevé d'interopérabilité entre eux. Afin de faciliter l'interopérabilité entre les SOC transfrontières, la Commission peut, au moyen d'actes d'exécution, après consultation de l'ECCC, préciser les conditions de cette interopérabilité. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.	***supprimé***

Or. en

Amendement 131
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 6 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Afin d'encourager l'échange d'informations entre les SOC transfrontières, ces derniers garantissent un niveau élevé d'interopérabilité entre eux. Afin de faciliter l'interopérabilité entre les SOC transfrontières, la Commission ***peut***, au moyen d'actes ***d'exécution***, ***après consultation de l'ECCC, préciser*** les conditions de cette interopérabilité. Ces actes ***d'exécution*** sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.	3. Afin d'encourager l'échange d'informations entre les SOC transfrontières ***et le secteur des ISAC***, ces derniers garantissent un niveau élevé d'interopérabilité entre eux ***et, dans la mesure du possible, avec ledit secteur***. Afin de faciliter l'interopérabilité entre les SOC transfrontières ***et le secteur des ISAC***, ***il convient d'harmoniser les normes et les protocoles de partage d'informations au regard des normes internationales et des meilleures pratiques du secteur. L'ECCC peut également demander à*** la Commission ***de proposer***, au moyen d'actes ***délégués, en étroite coordination avec les SOC régionaux et sur la base des normes internationales et des meilleures pratiques du secteur***, les conditions de cette interopérabilité. Ces actes ***délégués*** sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.

Or. en

Amendement 132
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 6 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Afin d'encourager l'échange d'informations entre les SOC transfrontières, ces derniers garantissent un	3. Afin d'encourager l'échange d'informations entre les SOC transfrontières, ces derniers garantissent un

niveau élevé d'interopérabilité entre eux. ***Afin de*** faciliter l'interopérabilité entre les SOC transfrontières, la Commission peut, au moyen d'actes d'exécution, après consultation de l'ECCC, préciser les conditions de cette interopérabilité. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.

niveau élevé d'interopérabilité entre eux. ***La passation conjointe de marchés en matière d'infrastructures, de services et d'outils cyber peut*** faciliter l'interopérabilité entre les SOC transfrontières***. Afin de préciser les conditions de l'interopérabilité des SOC transfrontières***, la Commission peut, au moyen d'actes d'exécution, après consultation de l'ECCC ***et de l'ENISA***, préciser les conditions de cette interopérabilité. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.

Or. en

Amendement 133
Evžen Tošenovský

Proposition de règlement
Article 6 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les SOC transfrontières concluent des accords de coopération entre eux, qui précisent les principes de partage d'informations en vigueur entre les plateformes transfrontières.	***supprimé***

Or. en

Amendement 134
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 6 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les SOC transfrontières concluent des accords de coopération entre eux, qui	4. Les SOC transfrontières concluent des accords de coopération entre eux, qui

précisent les principes de partage d'informations en vigueur entre les plateformes transfrontières.	précisent les principes de partage d'informations en vigueur entre les plateformes transfrontières***, en tenant compte des mécanismes de partage d'informations pertinents qui existent déjà en vertu de la directive (UE) 2022/2555***. ***Les mécanismes de partage d'informations relatives à un incident de cybersécurité majeur potentiel ou en cours sont conformes aux dispositions applicables au titre de la directive (UE) 2022/2555.***

Or. en

Amendement 135
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 6 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les SOC transfrontières concluent des accords de coopération entre eux, qui précisent les principes de partage d'informations en vigueur entre les plateformes transfrontières.	4. Les SOC transfrontières concluent des accords de coopération entre eux ***et avec les ISAC du secteur***, qui précisent les principes de partage d'informations ***et d'interopérabilité*** en vigueur entre les plateformes transfrontières.

Or. en

Amendement 136
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 7 – titre

Texte proposé par la Commission	*Amendement*
Coopération et partage d'informations avec ***les entités de l'Union***	Coopération et partage d'informations avec ***le réseau des CSIRT***

Or. en

Amendement 137
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 7 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ***ils fournissent*** sans retard injustifié les informations pertinentes à EU-CyCLONe, au réseau des CSIRT et à la Commission, compte tenu de leurs rôles respectifs en matière de gestion des crises conformément à la directive (UE) 2022/2555.	1. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours ***aux fins d'une appréciation commune de la situation***, ***le SOC coordinateur fournit*** sans retard injustifié les informations pertinentes à ***son CSIRT ou à une autorité compétente, qui, à son tour, les communiquera à*** EU-CyCLONe, au réseau des CSIRT et à la Commission, compte tenu de leurs rôles ***et procédures*** respectifs en matière de gestion des crises conformément à la directive (UE) 2022/2555.

Or. en

Justification

Dans le cas d'incidents majeurs, il est recommandé de s'en tenir à la procédure SRI 2.

Amendement 138
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 7 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils fournissent sans retard injustifié les informations pertinentes à EU-CyCLONe, au réseau des CSIRT ***et*** à la Commission, ***compte tenu de*** leurs rôles respectifs en matière de gestion des crises	1. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils fournissent sans retard injustifié les informations pertinentes à EU-CyCLONe, au réseau des CSIRT**,** à la Commission ***et à l'ENISA***, ***en vertu de*** leurs rôles respectifs en matière de gestion

conformément à la directive (UE) 2022/2555.	des crises conformément à la directive (UE) 2022/2555.

Or. en

Amendement 139
Evžen Tošenovský

Proposition de règlement
Article 7 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les ***SOC transfrontières*** obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils fournissent sans retard injustifié les informations pertinentes à EU-CyCLONe***,*** au réseau des CSIRT ***et à la Commission***, compte tenu de leurs rôles respectifs en matière de gestion des crises conformément à la directive (UE) 2022/2555.	1. Lorsque les ***CSIRT-ISAC*** obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils fournissent sans retard injustifié les informations pertinentes à EU-CyCLONe ***et*** au réseau des CSIRT, compte tenu de leurs rôles respectifs en matière de gestion des crises conformément à la directive (UE) 2022/2555.

Or. en

Amendement 140
Evžen Tošenovský

Proposition de règlement
Article 7 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La Commission peut, au moyen d'actes d'exécution, déterminer les dispositions procédurales du partage d'informations prévu au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.	***supprimé***

Or. en

Amendement 141
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 7 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La Commission peut, au moyen d'actes d'exécution, déterminer les dispositions procédurales du partage d'informations prévu au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.	2. La Commission peut, ***après consultation des plateformes transfrontières et du réseau CSIRT,*** au moyen d'actes d'exécution, déterminer les dispositions procédurales du partage d'informations prévu au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement ***ainsi qu'avec la directive (UE) 2022/2555***.

Or. en

Justification

Dans le cas d'incidents majeurs, il est recommandé de s'en tenir à la procédure SRI 2 et donc de consulter en premier lieu le réseau CSIRT.

Amendement 142
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 7 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La Commission peut, au moyen d'actes d'exécution, déterminer les dispositions procédurales du partage d'informations prévu au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.	2. La Commission peut***, après avoir consulté l'ENISA***, au moyen d'actes d'exécution, déterminer les dispositions procédurales du partage d'informations prévu au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.

Or. en

Amendement 143
Johan Nissinen

Proposition de règlement
Article 8 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres participant au cyberbouclier européen garantissent un niveau élevé de sécurité des données et de sécurité physique de l'infrastructure du cyberbouclier européen et ils veillent à ce que l'infrastructure soit gérée et contrôlée de manière adéquate de sorte qu'il soit possible de la protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, y compris celle des données échangées par l'intermédiaire de l'infrastructure.	1. Les États membres participant au cyberbouclier européen garantissent un niveau élevé ***de confidentialité,*** de sécurité des données et de sécurité physique de l'infrastructure du cyberbouclier européen et ils veillent à ce que l'infrastructure soit gérée et contrôlée de manière adéquate de sorte qu'il soit possible de la protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, y compris celle des données échangées par l'intermédiaire de l'infrastructure.

Or. en

Amendement 144
Evžen Tošenovský

Proposition de règlement
Article 8 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de	***supprimé***

sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.

Or. en

Amendement 145
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 8 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.	3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement***, la directive (UE) 2022/2555 et la directive (UE) 2022/2557***. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.

Or. en

Amendement 146
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 8 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres	3. La Commission peut***, après consultation de l'ENISA,*** adopter des actes d'exécution établissant des exigences

afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.	techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.

Or. en

Amendement 147
Johan Nissinen

Proposition de règlement
Article 9 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Un mécanisme d'urgence dans le domaine de la cybersécurité est mis en place afin d'améliorer la résilience de l'Union face aux cybermenaces majeures et d'anticiper et d'atténuer, dans un esprit de solidarité, les incidences à court terme des incidents de cybersécurité importants et majeurs (ci-après le «mécanisme»).	1. Un mécanisme d'urgence dans le domaine de la cybersécurité est mis en place afin d'améliorer la résilience de l'Union face aux cybermenaces majeures et d'anticiper et d'atténuer, dans un esprit de solidarité, les incidences à court terme des incidents de cybersécurité importants et majeurs (ci-après le «mécanisme»)***, à la demande explicite de l'État membre ou des États membres concernés***.

Or. en

Amendement 148
Evžen Tošenovský

Proposition de règlement
Article 9 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Un mécanisme d'urgence dans le	1. Un mécanisme d'urgence dans le

domaine de la cybersécurité est mis en place afin d'améliorer la résilience de l'Union face aux cybermenaces ***majeures*** et d'anticiper et d'atténuer, dans un esprit de solidarité, les incidences à court terme des incidents de cybersécurité importants et majeurs (ci-après le «mécanisme»).	domaine de la cybersécurité est mis en place afin d'améliorer la résilience de l'Union face aux cybermenaces ***importantes*** et d'anticiper et d'atténuer, dans un esprit de solidarité, les incidences à court terme des incidents de cybersécurité importants et majeurs (ci-après le «mécanisme»).

Or. en

Amendement 149
Johan Nissinen

Proposition de règlement
Article 10 – paragraphe 1 – point b

Texte proposé par la Commission	*Amendement*
b) les mesures de réaction, qui soutiennent la réaction aux incidents de cybersécurité importants et majeurs ainsi que le rétablissement immédiat, prévues par les fournisseurs de confiance participant à la réserve de cybersécurité de l'UE établie en vertu de l'article 12;	b) les mesures de réaction, qui soutiennent la réaction aux incidents de cybersécurité importants et majeurs ainsi que le rétablissement immédiat, prévues par les fournisseurs de confiance participant à la réserve de cybersécurité de l'UE établie en vertu de l'article 12***, à la demande explicite de l'État membre ou des États membres concernés***;

Or. en

Amendement 150
Evžen Tošenovský

Proposition de règlement
Article 10 – paragraphe 1 – point b

Texte proposé par la Commission	*Amendement*
b) les mesures de réaction, qui soutiennent la réaction aux incidents de cybersécurité importants et majeurs ainsi que le rétablissement immédiat, prévues par les fournisseurs de confiance participant à la réserve de cybersécurité de	b) les mesures de réaction, qui soutiennent la réaction aux incidents de cybersécurité importants et majeurs ainsi que le rétablissement immédiat, prévues par les fournisseurs ***de services de sécurité gérés*** de confiance participant à la réserve

l'UE établie en vertu de l'article 12;	de cybersécurité de l'UE établie en vertu de l'article 12;

Or. en

Amendement 151
Ville Niinistö
au nom du groupe Verts/ALE

Proposition de règlement
Article 10 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. À compter du déclenchement du mécanisme d'urgence dans le domaine de la cybersécurité, la Commission fait rapport chaque année sur son évaluation des points forts et des points faibles du fonctionnement du mécanisme, en indiquant notamment si des exigences supplémentaires en matière de coopération ou de formation sont nécessaires.

Or. en

Amendement 152
Evžen Tošenovský

Proposition de règlement
Article 11 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Aux fins de contribuer aux tests de préparation coordonnés des entités visés à l'article 10, paragraphe 1, point a), dans l'ensemble de l'Union, la Commission, après consultation du groupe de coopération SRI et de l'ENISA, recense les secteurs ou sous-secteurs concernés, dans les secteurs hautement critiques énumérés à l'annexe I de la directive (UE) 2022/2555, dont les entités peuvent être soumises à des	1. Aux fins de contribuer aux tests de préparation coordonnés des entités visés à l'article 10, paragraphe 1, point a), dans l'ensemble de l'Union, la Commission, après consultation du groupe de coopération SRI et de l'ENISA, recense les secteurs ou sous-secteurs concernés, dans les secteurs hautement critiques énumérés à l'annexe I de la directive (UE) 2022/2555, dont les entités peuvent être soumises à des

tests de préparation coordonnés, en tenant compte des évaluations coordonnées des risques et des tests de résilience existants et prévus au niveau de l'Union.	tests de préparation coordonnés ***volontaires***, en tenant compte des évaluations coordonnées des risques et des tests de résilience existants et prévus au niveau de l'Union.

Or. en

Amendement 153
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 11 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le groupe de coopération SRI, en collaboration avec la Commission, l'ENISA et le haut représentant, élabore des scénarios de risque et des méthodologies communs pour les ***exercices de*** tests coordonnés.	2. Le groupe de coopération SRI, en collaboration avec la Commission, l'ENISA et le haut représentant, élabore des scénarios de risque et des méthodologies communs pour les tests ***de préparation*** coordonnés***. Cela permettra de recenser les secteurs ou sous-secteurs concernés dans lesquels les entités peuvent être soumises aux tests de préparation coordonnés décrits au paragraphe 1***.

Or. en

Amendement 154
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 11 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le groupe de coopération SRI, en collaboration avec la Commission, l'ENISA ***et*** le haut représentant, élabore des scénarios de risque et des méthodologies communs pour les exercices de tests coordonnés.	2. Le groupe de coopération SRI, en collaboration avec la Commission, l'ENISA***,*** le haut représentant ***et les entités susceptibles d'être soumises à des tests de préparation***, élabore des scénarios de risque et des méthodologies communs pour

les exercices de tests coordonnés.

Or. en

Amendement 155
Johan Nissinen

Proposition de règlement
Article 12 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Une réserve de cybersécurité de l'Union est créée afin d'aider les utilisateurs visés au paragraphe 3 à réagir aux incidents de cybersécurité importants ou majeurs, ou à fournir une assistance à cet effet, et à favoriser le rétablissement immédiat après de tels incidents.	1. Une réserve de cybersécurité de l'Union est créée afin d'aider les utilisateurs visés au paragraphe 3 à réagir aux incidents de cybersécurité importants ou majeurs, ou à fournir une assistance à cet effet, et à favoriser le rétablissement immédiat après de tels incidents***, à la demande explicite de l'État membre ou des États membres concernés et sans préjudice du caractère spécifique de la politique de sécurité et de défense de certains États membres***.

Or. en

Amendement 156
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 12 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les services peuvent être déployés dans tous les États membres.	2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les services peuvent être déployés dans tous les États membres***, renforcer la résilience et la souveraineté***

de l'Union et en améliorer la compétitivité. Les noms des fournisseurs de confiance sélectionnés et les services qu'ils fournissent sont tenus confidentiels.

Or. en

Amendement 157
Johan Nissinen

Proposition de règlement
Article 12 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les services peuvent être déployés dans tous les États membres.	2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les services peuvent être déployés dans tous les États membres. ***La réserve de cybersécurité de l'Union ne limite pas la nécessité d'autoriser les pays à analyser et à évaluer leurs propres besoins.***

Or. en

Amendement 158
Evžen Tošenovský

Proposition de règlement
Article 12 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les services peuvent être	2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs ***de services de sécurité gérés*** de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les

déployés dans tous les États membres.	services peuvent être déployés dans tous les États membres***, à leur demande***.

Or. en

Amendement 159
Evžen Tošenovský

Proposition de règlement
Article 12 – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
b) les ***institutions, organes et organismes de l'Union***.	b) les ***pays tiers visés à l'article 17 du présent règlement***.

Or. en

Amendement 160
Evžen Tošenovský

Proposition de règlement
Article 12 bis – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les utilisateurs visés au paragraphe 3, point a), ***ont*** recours aux services de la réserve de cybersécurité de l'Union afin de réagir aux incidents importants ou majeurs touchant des entités actives dans des secteurs critiques ou hautement critiques, ou de fournir une assistance à cet effet et de favoriser le rétablissement immédiat.	4. Les utilisateurs visés au paragraphe 3, point a), ***peuvent avoir*** recours aux services de la réserve de cybersécurité de l'Union***, à leur demande,*** afin de réagir aux incidents importants ou majeurs touchant des entités actives dans des secteurs critiques ou hautement critiques, ou de fournir une assistance à cet effet et de favoriser le rétablissement immédiat.

Or. en

Amendement 161
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement

Article 12 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission a la responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission définit les priorités et l'évolution de la réserve de cybersécurité de l'Union, conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres actions et programmes de l'Union.	5. La Commission a la responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission définit les priorités et l'évolution de la réserve de cybersécurité de l'Union***, en coordination avec le groupe de coopération SRI 2***, ***et*** conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres actions et programmes de l'Union.

Or. en

Amendement 162
Evžen Tošenovský

Proposition de règlement
Article 12 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission a la responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission définit les priorités et l'évolution de la réserve de cybersécurité de l'Union, conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres actions et programmes de l'Union.	5. La Commission a la responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission***, en collaboration avec l'ENISA,*** définit les priorités et l'évolution de la réserve de cybersécurité de l'Union, conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres actions et programmes de l'Union.

Or. en

Amendement 163
Evžen Tošenovský

Proposition de règlement
Article 12 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. La Commission peut confier, par voie de conventions de contribution, le fonctionnement et l'administration de la réserve de cybersécurité de l'UE, en tout ou en partie, à l'ENISA.	***supprimé***

Or. en

Amendement 164
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 12 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. La Commission ***peut confier***, par voie de conventions de contribution, le fonctionnement et l'administration de la réserve de cybersécurité de l'UE, en tout ou en partie, à l'ENISA.	6. La Commission ***confie***, par voie de conventions de contribution, le fonctionnement et l'administration de la réserve de cybersécurité de l'UE, en tout ou en partie, à l'ENISA.

Or. en

Amendement 165
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 12 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité	7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité

de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres et de la Commission. L'ENISA établit une autre carte similaire, après consultation de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.	de l'UE, l'ENISA élabore une cartographie des services nécessaires, ***notamment des compétences et des capacités recherchées auprès de la main-d'œuvre dans le domaine de la cybersécurité,*** après consultation des États membres et de la Commission. L'ENISA établit une autre carte similaire, après consultation de la Commission ***et en collaboration avec le secteur privé***, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.

Or. en

Amendement 166
Evžen Tošenovský

Proposition de règlement
Article 12 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres et de la Commission. L'ENISA établit une autre carte similaire, après consultation de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.	7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres et de la Commission. L'ENISA établit une autre carte similaire, après consultation de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant. ***Elle informe également le Conseil de leurs besoins.***

Or. en

Amendement 167
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement

Article 12 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres ***et*** de la Commission. L'ENISA établit une autre carte similaire, après consultation de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.	7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres***,*** de la Commission***, des fournisseurs de services de sécurité gérés et des représentants du secteur***. L'ENISA établit une autre carte similaire, après consultation de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.

Or. en

Amendement 168
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 12 – paragraphe 8

Texte proposé par la Commission	*Amendement*
8. La Commission peut***, au moyen d'actes d'exécution,*** préciser les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2.	8. La Commission peut ***adopter un acte délégué en conformité avec l'article 20 bis du présent règlement afin de*** préciser les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2.

Or. en

Amendement 169
Evžen Tošenovský

Proposition de règlement
Article 13 – paragraphe 5 – point a

Texte proposé par la Commission	*Amendement*
a) ***des informations appropriées concernant l'entité*** touchée et les répercussions potentielles de l'incident, ainsi que l'utilisation prévue de l'aide demandée, y compris une indication des besoins estimés;	a) ***le type d'entité*** touchée et les répercussions potentielles de l'incident, ainsi que l'utilisation prévue de l'aide demandée, y compris une indication des besoins estimés;

Or. en

Amendement 170
Evžen Tošenovský

Proposition de règlement
Article 13 – paragraphe 5 – point b

Texte proposé par la Commission	*Amendement*
b) des informations sur les mesures prises pour atténuer l'incident pour lequel l'aide a été demandée, visées au paragraphe 2;	b) des informations ***générales*** sur les mesures prises pour atténuer l'incident pour lequel l'aide a été demandée, visées au paragraphe 2;

Or. en

Amendement 171
Evžen Tošenovský

Proposition de règlement
Article 13 – paragraphe 5 – point c

Texte proposé par la Commission	*Amendement*
c) des informations sur les autres formes d'aide dont dispose l'entité touchée***, y compris les dispositions contractuelles en vigueur relatives aux services de réaction aux incidents et de rétablissement immédiat, ainsi que les contrats d'assurance couvrant potentiellement ce type d'incident***.	c) des informations sur les autres formes d'aide dont dispose l'entité touchée.

Or. en

Amendement 172
Evžen Tošenovský

Proposition de règlement
Article 13 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. La Commission peut, au moyen d'actes d'exécution, préciser davantage les modalités d'attribution des services d'aide fournis par la réserve de cybersécurité de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2.	***supprimé***

Or. en

Amendement 173
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 13 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. La Commission peut***, au moyen d'actes d'exécution,*** préciser davantage les modalités d'attribution des services d'aide fournis par la réserve de cybersécurité de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2.	7. La Commission peut ***adopter des actes délégués en conformité avec l'article 20 bis du présent règlement afin de*** préciser davantage les modalités d'attribution des services d'aide fournis par la réserve de cybersécurité de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2.

Or. en

Amendement 174

Evžen Tošenovský

Proposition de règlement
Article 14 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les demandes d'aide adressées à la réserve de cybersécurité de l'Union sont évaluées par la Commission, assistée par l'ENISA ***ou selon les modalités définies dans les conventions de contribution visées à l'article 12, paragraphe 6***, et ***une réponse*** est transmise ***dans les meilleurs délais*** aux utilisateurs visés à l'article 12, paragraphe 3.	1. Les demandes d'aide adressées à la réserve de cybersécurité de l'Union sont évaluées par la Commission, assistée par l'ENISA, et ***sa décision*** est transmise ***sans retard injustifié*** aux utilisateurs visés à l'article 12, paragraphe 3***, et en tout état de cause dans les 24 heures***.

Or. en

Amendement 175
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 14 – paragraphe 2 – point d

Texte proposé par la Commission	*Amendement*
d) la nature transfrontière potentielle de l'incident et le risque de propagation à d'autres États membres ou utilisateurs;	d) ***l'ampleur et*** la nature transfrontière potentielle de l'incident et le risque de propagation à d'autres États membres ou utilisateurs;

Or. en

Amendement 176
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 14 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les services de la réserve de cybersécurité de l'UE sont fournis	3. Les services de la réserve de cybersécurité de l'UE sont fournis

conformément à des accords spécifiques conclus entre le fournisseur de services et l'utilisateur bénéficiant de l'aide de la réserve de cybersécurité de l'UE. Ces accords contiennent des conditions de responsabilité.	conformément à des accords spécifiques conclus entre le fournisseur de services et l'utilisateur bénéficiant de l'aide de la réserve de cybersécurité de l'UE. Ces accords contiennent des conditions de responsabilité ***et toute autre disposition que les parties à l'accord jugent nécessaire à la fourniture du service concerné***.

Or. en

Amendement 177
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 14 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les services de la réserve de cybersécurité de l'UE sont fournis conformément à des accords spécifiques conclus entre le fournisseur de services et l'utilisateur bénéficiant de l'aide de la réserve de cybersécurité de l'UE. Ces accords contiennent des conditions de responsabilité.	3. Les services de la réserve de cybersécurité de l'UE sont fournis ***avec l'accord de l'utilisateur et*** conformément à des accords spécifiques conclus entre le fournisseur de services et l'utilisateur bénéficiant de l'aide de la réserve de cybersécurité de l'UE. Ces accords contiennent des conditions de responsabilité.

Or. en

Amendement 178
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 14 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les accords visés au paragraphe 3 ***peuvent se baser*** sur des modèles élaborés par l'ENISA, après consultation des États membres.	4. Les accords visés au paragraphe 3 ***se fondent*** sur des modèles élaborés par l'ENISA, après consultation des États membres ***et des autres utilisateurs de la***

réserve.

Or. en

Amendement 179
Evžen Tošenovský

Proposition de règlement
Article 14 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission et l'ENISA ne sont pas contractuellement responsables des dommages causés à des tiers par les services fournis dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'UE.	***supprimé***

Or. en

Amendement 180
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 14 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission et l'ENISA ne sont pas contractuellement responsables des dommages causés à des tiers par les services fournis dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'UE.	5. La Commission et l'ENISA ne sont pas contractuellement responsables des dommages causés à des tiers par les services fournis dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'UE***, sauf en cas de négligence lors de l'évaluation de la demande du fournisseur de services, ou dans les cas où la Commission ou l'ENISA sont elles-mêmes utilisatrices et sont jugées responsables des dommages***.

Or. en

Amendement 181
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 14 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission et l'ENISA ne sont pas contractuellement responsables des dommages causés à des tiers par les services fournis dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'UE.	5. La Commission et l'ENISA ne sont pas contractuellement responsables des dommages causés à des tiers par les services fournis dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'UE***, sauf pour les cas où la Commission ou l'ENISA sont des utilisateurs de la réserve conformément à l'article 14, paragraphe 3***.

Or. en

Amendement 182
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 14 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Au plus tard un mois après avoir bénéficié de l'aide de la réserve, l'utilisateur présente à la Commission et à l'ENISA un rapport de synthèse sur le service fourni, les résultats obtenus et les enseignements tirés. Lorsque l'utilisateur est originaire d'un pays tiers conformément aux dispositions de l'article 17, ce rapport est également communiqué au haut représentant.	6. Au plus tard un mois après avoir bénéficié de l'aide de la réserve, l'utilisateur présente à la Commission et à l'ENISA un rapport de synthèse sur le service fourni, les résultats obtenus et les enseignements tirés. Lorsque l'utilisateur est originaire d'un pays tiers conformément aux dispositions de l'article 17, ce rapport est également communiqué au haut représentant. ***Le rapport respecte le droit de l'Union ou le droit national relatif à la protection des informations sensibles ou classifiées.***

Or. en

Amendement 183
Evžen Tošenovský

Proposition de règlement
Article 14 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Au plus tard un mois après avoir bénéficié de l'aide de la réserve, l'utilisateur présente à la Commission ***et*** à l'ENISA un rapport de synthèse sur le service fourni, les résultats obtenus et les enseignements tirés. Lorsque l'utilisateur est originaire d'un pays tiers conformément aux dispositions de l'article 17, ce rapport est également communiqué au haut représentant.	6. Au plus tard un mois après avoir bénéficié de l'aide de la réserve, l'utilisateur présente à la Commission***,*** à l'ENISA***, au réseau des CSIRT et, le cas échéant, à EU-CyCLONe,*** un rapport de synthèse sur le service fourni, les résultats obtenus et les enseignements tirés. Lorsque l'utilisateur est originaire d'un pays tiers conformément aux dispositions de l'article 17, ce rapport est également communiqué au haut représentant.

Or. en

Amendement 184
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 14 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. La Commission fait régulièrement rapport au groupe de coopération SRI sur l'utilisation de cette aide et les résultats obtenus.	7. La Commission fait régulièrement rapport au groupe de coopération SRI sur l'utilisation de cette aide et les résultats obtenus. ***Il protège les informations confidentielles, conformément au droit de l'Union ou au droit national relatif à la protection des informations sensibles ou classifiées.***

Or. en

Amendement 185
Evžen Tošenovský

Proposition de règlement

Article 14 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. La Commission fait ***régulièrement*** rapport au groupe de coopération SRI sur l'utilisation de cette aide et les résultats obtenus.	7. La Commission fait rapport ***au moins deux fois par an*** au groupe de coopération SRI sur l'utilisation de cette aide et les résultats obtenus.

Or. en

Amendement 186
Evžen Tošenovský

Proposition de règlement
Article 15 – titre

Texte proposé par la Commission	*Amendement*
Coordination avec les mécanismes de gestion des crises	Coordination ***du mécanisme d'urgence dans le domaine de la cybersécurité*** avec les mécanismes de gestion des crises

Or. en

Amendement 187
Evžen Tošenovský

Proposition de règlement
Article 15 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. En consultation avec le haut représentant, le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter l'assistance fournie dans le cadre de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune***, y compris par l'intermédiaire des équipes d'intervention rapide en cas d'incident informatique***. ***Il peut également s'ajouter ou contribuer à l'assistance fournie par un État membre à un autre***	3. En consultation avec le haut représentant, le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter l'assistance fournie dans le cadre de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune.

dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne.

Or. en

Amendement 188
Evžen Tošenovský

Proposition de règlement
Article 16 – titre

Texte proposé par la Commission	*Amendement*
Fournisseurs de confiance	Fournisseurs de ***services de sécurité gérés de*** confiance

Or. en

Amendement 189
Johan Nissinen

Proposition de règlement
Article 16 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. Dans les procédures de passation de marchés menées pour la création de la réserve de cybersécurité de l'UE, le pouvoir adjudicateur agit conformément aux principes énoncés dans le règlement (UE, Euratom) 2018/1046 et aux principes suivants:	1. Dans les procédures de passation de marchés menées pour la création de la réserve de cybersécurité de l'UE, le pouvoir adjudicateur agit conformément aux principes énoncés dans le règlement (UE, Euratom) 2018/1046***, sans préjudice de la responsabilité première des États membres dans le domaine de la sécurité nationale,*** et ***conformément*** aux principes suivants:

Or. en

Amendement 190
Evžen Tošenovský

Proposition de règlement
Article 16 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) la réserve de cybersécurité de l'UE comprend des services qui peuvent être déployés dans tous les États membres, compte tenu en particulier des exigences nationales relatives à la fourniture de ces services, y compris la certification ou l'accréditation;	a) la réserve de cybersécurité de l'UE comprend des services qui peuvent être déployés dans tous les États membres ***et les pays tiers en conformité avec l'article 17 du présent règlement***, compte tenu en particulier des exigences nationales relatives à la fourniture de ces services, y compris la certification ou l'accréditation;

Or. en

Amendement 191
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 16 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) la réserve de cybersécurité de l'UE apporte une valeur ajoutée européenne, en contribuant à la réalisation des objectifs énoncés à l'article 3 du règlement (UE) 2021/694, y compris la promotion du développement des compétences en matière de cybersécurité dans l'UE.	c) la réserve de cybersécurité de l'UE apporte une valeur ajoutée européenne, en contribuant à la réalisation des objectifs énoncés à l'article 3 du règlement (UE) 2021/694, y compris la promotion du développement des compétences en matière de cybersécurité dans l'UE***, le renforcement de la résilience et de la souveraineté de l'Union, ainsi que l'amélioration de la compétitivité de l'Union***.

Or. en

Amendement 192
Evžen Tošenovský

Proposition de règlement
Article 16 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) la réserve de cybersécurité de l'UE ***apporte une valeur ajoutée européenne, en contribuant*** à la réalisation des objectifs énoncés à l'article 3 du règlement (UE) 2021/694, y compris la promotion du développement des compétences en matière de cybersécurité dans l'UE.	c) la réserve de cybersécurité de l'UE ***contribue*** à la réalisation des objectifs énoncés à l'article 3 du règlement (UE) 2021/694, y compris la promotion du développement des compétences en matière de cybersécurité dans l'UE.

Or. en

Amendement 193
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 16 – paragraphe 2 – point f

Texte proposé par la Commission	*Amendement*
f) le fournisseur possède l'équipement technique matériel et logiciel nécessaire au service demandé;	f) le fournisseur possède l'équipement technique matériel et logiciel ***de pointe*** nécessaire au service demandé ***et satisfait, le cas échéant, aux exigences énoncées dans le règlement XX/XXXX (loi sur la cyberrésilience)***;

Or. en

Amendement 194
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 16 – paragraphe 2 – point f bis (nouveau)

Texte proposé par la Commission	*Amendement*
	f bis) le fournisseur démontre que ses structures de décision et de gestion sont exemptes de toute influence indue de la part de gouvernements d'États recensés en tant que rivaux systémiques de

l'Union;

Or. en

Amendement 195
Evžen Tošenovský

Proposition de règlement
Article 16 – paragraphe 2 – point h

Texte proposé par la Commission	*Amendement*
h) le fournisseur est en mesure de fournir le service dans un bref délai dans le ou les États membres où il peut le faire;	h) le fournisseur est en mesure de fournir le service dans un bref délai dans le ou les États membres ***ou pays tiers*** où il peut le faire;

Or. en

Amendement 196
Evžen Tošenovský

Proposition de règlement
Article 16 – paragraphe 2 – point i

Texte proposé par la Commission	*Amendement*
i) le fournisseur est en mesure de fournir le service dans la langue locale du ou des États membres où il peut le faire;	i) le fournisseur est en mesure de fournir le service dans la langue locale du ou des États membres ***ou pays tiers*** où il peut le faire ***ou dans l'une des langues de travail des institutions de l'Union***;

Or. en

Amendement 197
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 16 – paragraphe 2 – point j

Texte proposé par la Commission	*Amendement*
j) dès qu'un schéma de certification de l'UE pour les services de sécurité gérés conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma.	j) dès qu'un schéma de certification de l'UE pour les services de sécurité gérés conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma***, dans un délai de deux ans à compter de l'adoption du schéma***.

Or. en

Amendement 198
Evžen Tošenovský

Proposition de règlement
Article 16 – paragraphe 2 – point j

Texte proposé par la Commission	*Amendement*
j) dès qu'un schéma de certification de ***l'UE*** pour les services de sécurité gérés conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma.	j) dès qu'un schéma de certification de ***cybersécurité de l'Union*** pour les services de sécurité gérés conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma.

Or. en

Amendement 199
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 16 – paragraphe 2 – point j

Texte proposé par la Commission	*Amendement*
j) dès qu'un schéma de certification de l'UE pour les services de sécurité gérés conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma.	j) dès qu'un schéma de certification de l'UE pour les services de sécurité gérés conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma ***dans un délai de deux ans***.

Or. en

Justification

La proposition de la Commission prévoit qu'un schéma de certification vienne se substituer aux exigences techniques énoncées dans le présent règlement. Cet amendement accorde un délai supplémentaire aux entreprises, en particulier aux PME, pour adopter ce schéma, favorisant ainsi des conditions de concurrence plus équitables dans l'ensemble de l'Union. Dans l'intervalle, elles devront se conformer aux exigences techniques du présent règlement.

Amendement 200
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 16 – paragraphe 2 – point j bis (nouveau)

Texte proposé par la Commission	*Amendement*
	j bis) le fournisseur est en mesure de dissocier ses services du contrat plus large, de sorte que l'utilisateur puisse opter pour un autre fournisseur de services.

Or. en

Amendement 201
Evžen Tošenovský

Proposition de règlement
Article 17 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. La Commission et le haut représentant se coordonnent en ce qui concerne les demandes reçues et la mise en œuvre de l'aide accordée aux pays tiers au titre de la réserve de cybersécurité de l'UE.	6. La Commission et le haut représentant ***informent le Conseil sans retard injustifié et*** se coordonnent en ce qui concerne les demandes reçues et la mise en œuvre de l'aide accordée aux pays tiers au titre de la réserve de cybersécurité de l'UE.

Or. en

Amendement 202
Evžen Tošenovský

Proposition de règlement
Article 18

Texte proposé par la Commission	*Amendement*
Article 18	***supprimé***
Mécanisme d'analyse des incidents de cybersécurité	
1. À la demande de la Commission, d'EU-CyCLONe ou du réseau des CSIRT, l'ENISA analyse et évalue les menaces, les vulnérabilités et les mesures d'atténuation d'un incident de cybersécurité important ou majeur spécifique. Après l'analyse et l'évaluation d'un incident, l'ENISA remet un rapport d'analyse au réseau des CSIRT, à EU-CyCLONe et à la Commission afin de les aider à s'acquitter de leurs tâches, compte tenu notamment de celles énoncées aux articles 15 et 16 de la directive (UE) 2022/2555. Le cas échéant, la Commission transmet le rapport au haut représentant.	
2. Pour préparer le rapport d'analyse visé au paragraphe 1, l'ENISA collabore avec toutes les parties prenantes concernées, y compris les représentants des États membres, la Commission, les autres institutions, organes et organismes concernés de l'UE, les fournisseurs de services de sécurité gérés et les utilisateurs de services de cybersécurité. Le cas échéant, l'ENISA collabore également avec les entités touchées par des incidents de cybersécurité importants ou majeurs. Pour étayer l'analyse, l'ENISA peut également consulter d'autres types de parties prenantes. Les représentants consultés déclarent tout conflit d'intérêts potentiel.	
3. Le rapport comprend une analyse et un examen de l'incident de cybersécurité important ou majeur, y compris des principales causes, vulnérabilités et enseignements tirés. Il protège les	

informations confidentielles, conformément au droit de l'Union ou au droit national relatif à la protection des informations sensibles ou classifiées.

4. Le cas échéant, le rapport formule des recommandations afin d'améliorer la posture cyber de l'Union.

5. Si possible, une version du rapport est rendue publique. Cette version contient uniquement des informations publiques.

Or. en

Amendement 203
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 18 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Pour préparer le rapport d'analyse visé au paragraphe 1, l'ENISA collabore avec toutes les parties prenantes concernées, y compris les représentants des États membres, la Commission, les autres institutions, organes et organismes concernés de l'UE, les fournisseurs de services de sécurité gérés et les utilisateurs de services de cybersécurité. Le cas échéant, l'ENISA collabore également avec les entités touchées par des incidents de cybersécurité importants ou majeurs. Pour étayer l'analyse, l'ENISA peut également consulter d'autres types de parties prenantes. Les représentants consultés déclarent tout conflit d'intérêts potentiel.	2. Pour préparer le rapport d'analyse visé au paragraphe 1, l'ENISA collabore avec toutes les parties prenantes concernées, y compris les représentants des États membres, la Commission, les autres institutions, organes et organismes concernés de l'UE, les fournisseurs de services de sécurité gérés et les utilisateurs de services de cybersécurité***, et recueille leurs retours d'informations***. Le cas échéant, l'ENISA collabore également avec les entités touchées par des incidents de cybersécurité importants ou majeurs. Pour étayer l'analyse, l'ENISA peut également consulter d'autres types de parties prenantes. Les représentants consultés déclarent tout conflit d'intérêts potentiel.

Or. en

Amendement 204

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposition de règlement
Article 18 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Le rapport comprend une analyse et un examen de l'incident de cybersécurité important ou majeur, y compris des principales causes, vulnérabilités et enseignements tirés. Il protège les informations confidentielles, conformément au droit de l'Union ou au droit national relatif à la protection des informations sensibles ou classifiées.	3. Le rapport comprend une analyse et un examen de l'incident de cybersécurité important ou majeur, y compris des principales causes, vulnérabilités et enseignements tirés. Il protège les informations confidentielles, conformément au droit de l'Union ou au droit national relatif à la protection des informations sensibles ou classifiées. ***Il ne comporte pas de précisions relatives aux vulnérabilités activement exploitées qui n'ont pas encore été corrigées.***

Or. en

Amendement 205
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 18 bis – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Le cas échéant, le rapport formule des recommandations afin d'améliorer la posture cyber de l'Union.	4. Le cas échéant, le rapport formule des recommandations ***concrètes, également à l'intention de toutes les parties prenantes,*** afin d'améliorer la posture cyber de l'Union.

Or. en

Amendement 206
Johan Nissinen

Proposition de règlement
Article 18 bis – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Le cas échéant, le rapport formule des recommandations afin d'améliorer la posture cyber de l'Union.	4. Le cas échéant, le rapport formule des recommandations ***volontaires non contraignantes d'un point de vue juridique*** afin d'améliorer la posture cyber de l'Union.

Or. en

Amendement 207
Evžen Tošenovský

Proposition de règlement
Article 19 – alinéa 1 – point 1 – sous-point a 1
Règlement (UE) 2021/694
Article 1 – paragraphe 1 – point a bis

Texte proposé par la Commission	*Amendement*
«a bis) soutenir le développement d'un cyberbouclier européen, y compris la mise au point, le déploiement et l'exploitation de ***plateformes*** SOC ***nationales et transfrontières*** qui contribuent à l'appréciation de la situation dans l'Union et au renforcement des capacités en matière de renseignement sur les cybermenaces de l'Union;»;	«a bis) soutenir le développement d'un cyberbouclier européen, y compris la mise au point, le déploiement et l'exploitation de ***CSIRT-ISAC et de*** SOC qui contribuent à l'appréciation de la situation dans l'Union et au renforcement des capacités en matière de renseignement sur les cybermenaces de l'Union;»;

Or. en

Amendement 208
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 19 – alinéa 1 – point 3
Règlement (UE) 2021/694
Article 14 – paragraphe 2

Texte proposé par la Commission	*Amendement*
Le programme peut octroyer un financement sous l'une ou l'autre des	Le programme peut octroyer un financement sous l'une ou l'autre des

formes prévues dans le règlement financier, y compris en particulier par la passation de marchés en premier lieu, ou des subventions et des prix.	formes prévues dans le règlement financier, y compris en particulier par la passation de marchés en premier lieu, ou des subventions et des prix. ***L'ENISA reçoit des ressources additionnelles pour mener à bien les tâches supplémentaires qui lui ont été confiées et qui sont définies dans le règlement XX/XXX (règlement sur la cyber-solidarité). Ces financements supplémentaires ne compromettent pas la réalisation des objectifs du programme.***

Or. en

Amendement 209
Evžen Tošenovský

Proposition de règlement
Article 19 – alinéa 1 – point 5
Règlement (UE) 2021/694
Article 19

Texte proposé par la Commission	*Amendement*
L'aide sous forme de subventions peut être octroyée directement par l'ECCC sans appel à propositions aux ***SOC nationaux*** visés à l'article 4 du règlement XXXX et ***au consortium d'hébergement visé*** à l'article 5 du règlement XXXX, conformément à l'article 195, paragraphe 1, point d), du règlement financier.	L'aide sous forme de subventions peut être octroyée directement par l'ECCC sans appel à propositions aux ***CSIRT-ISAC*** visés à l'article 4 du règlement XXXX et à l'article 5 du règlement XXXX, conformément à l'article 195, paragraphe 1, point d), du règlement financier.

Or. en

Amendement 210
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 20 – titre

Texte proposé par la Commission	*Amendement*

Évaluation

Évaluation ***et réexamen***

Or. en

Amendement 211
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 20 – alinéa 1

Texte proposé par la Commission	*Amendement*
Au plus tard le [***quatre*** ans après la date d'application du présent règlement], la Commission présente au Parlement européen et au Conseil ***un rapport sur l'évaluation et le réexamen du présent règlement***.	Au plus tard le [***deux*** ans après la date d'application du présent règlement] ***et tous les deux ans par la suite***, la Commission ***procède à une évaluation du fonctionnement des mesures définies dans le présent règlement et*** présente ***un rapport*** au Parlement européen et au Conseil. ***Cette évaluation porte, en particulier, sur les aspects suivants:*** ***a) la participation des États membres au cyberbouclier européen, notamment le nombre de SOC nationaux et transfrontières établis en vertu du présent règlement, ainsi que l'efficacité de l'échange d'informations;*** ***b) la contribution du présent règlement au renforcement de la résilience et de la souveraineté de l'Union, ainsi qu'à l'amélioration de la compétitivité des secteurs industriels concernés, y compris les PME, et au développement des compétences en matière de cybersécurité dans l'Union;*** ***c) l'utilisation de la réserve de cybersécurité, et notamment la question de savoir si le champ de la réserve devrait être élargi aux services de préparation aux incidents ou aux exercices communs qui réunissent les fournisseurs de confiance et les utilisateurs potentiels de la réserve de cybersécurité afin de***

	garantir, le cas échéant, le bon fonctionnement de la réserve;
	d) la contribution du présent règlement au développement et à l'amélioration des aptitudes et des compétences de la main-d'œuvre dans le secteur de la cybersécurité, qui sont indispensables pour renforcer la capacité de l'Union à détecter et à prévenir les menaces et les incidents de cybersécurité, à y réagir et à s'en rétablir;
	e) la contribution du présent règlement au déploiement et au développement de technologies de pointe dans l'Union.
	En fonction de ce rapport, la Commission présente au Parlement et au Conseil, le cas échéant, une proposition législative de modification du présent règlement.

Or. en

Amendement 212
Evžen Tošenovský

Proposition de règlement
Article 20 – alinéa 1

Texte proposé par la Commission	*Amendement*
Au plus tard le [quatre ans après la date d'application du présent règlement], la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement.	Au plus tard le [quatre ans après la date d'application du présent règlement], la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. ***Ce rapport est accompagné, s'il y a lieu, d'une proposition législative.***

Or. en

Amendement 213
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Proposition de règlement
Article 20 – alinéa 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Chaque année, lors de la présentation du projet de budget pour l'année suivante, la Commission soumet une évaluation détaillée des tâches confiées à l'ENISA en vertu du présent règlement et de la [proposition de règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques], ainsi que d'autres textes législatifs de l'Union, et précise les ressources financières et humaines nécessaires à l'accomplissement de ces tâches.

Or. en

Amendement 214
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposition de règlement
Article 20 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 20 bis
	Exercice de la délégation
	1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
	2. Le pouvoir d'adopter des actes délégués visé à l'article 12, paragraphe 8, et à l'article 13, paragraphe 7, […] est conféré à la Commission pour une période de cinq ans à compter du ... [date d'entrée en vigueur de l'acte législatif de base ou toute autre date fixée par les colégislateurs]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée

identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 12, paragraphe 8, et à l'article 13, paragraphe 7, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 12, paragraphe 8, et de l'article 13, paragraphe 7, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de [deux mois] à l'initiative du Parlement européen ou du Conseil.

Or. en

Amendement 215
Evžen Tošenovský

Proposition de règlement
Annexe I – alinéa 1 – point 1
Règlement (UE) 2021/694
Annexe I – section «Objectif spécifique nº 3 — Cybersécurité et confiance»

Texte proposé par la Commission	*Amendement*
1. Un co-investissement avec les États membres dans des équipements, des infrastructures et des savoir-faire avancés en matière de cybersécurité qui sont essentiels pour protéger les infrastructures critiques et le marché unique numérique dans son ensemble. Un tel co-investissement pourrait comprendre des investissements dans des installations quantiques et des ressources de données pour la cybersécurité, l'appréciation de la situation dans le cyberespace, notamment des SOC nationaux ***et des SOC transfrontières*** constituant le cyberbouclier européen; ainsi que d'autres outils à mettre à la disposition des secteurs public et privé dans toute l'Europe.	1. Un co-investissement avec les États membres dans des équipements, des infrastructures et des savoir-faire avancés en matière de cybersécurité qui sont essentiels pour protéger les infrastructures critiques et le marché unique numérique dans son ensemble. Un tel co-investissement pourrait comprendre des investissements dans des installations quantiques et des ressources de données pour la cybersécurité, l'appréciation de la situation dans le cyberespace, notamment des ***CSIRT et des*** SOC nationaux constituant le cyberbouclier européen; ainsi que d'autres outils à mettre à la disposition des secteurs public et privé dans toute l'Europe.

Or. en

Amendement 216
Evžen Tošenovský

Proposition de règlement
Annexe I – alinéa 1 – point 1
Règlement (UE) 2021/694
Annexe I – section «Objectif spécifique nº 3 — Cybersécurité et confiance»

Texte proposé par la Commission	*Amendement*
5. La promotion de la solidarité entre les États membres en ce qui concerne la préparation et la réaction aux incidents majeurs de cybersécurité par le déploiement de services de cybersécurité par-delà les frontières, y compris un soutien à l'assistance mutuelle entre les autorités publiques et la création d'une réserve de fournisseurs de services de	5. La promotion de la solidarité entre les États membres en ce qui concerne la préparation et la réaction aux incidents majeurs de cybersécurité par le déploiement de services de cybersécurité par-delà les frontières, y compris un soutien à l'assistance mutuelle entre les autorités publiques et la création d'une réserve de fournisseurs de services de

cybersécurité de confiance au niveau de l'Union.»;

sécurité gérés de confiance au niveau de l'Union.»;

Or. en